kaspersky

Kaspersky Basic | Standard | Plus | Premium

Innhold

Innlevering av data

Denne delen inneholder informasjon om de spesifikke dataene du gir til Kaspersky mens du bruker programmet. Underdelen Lagring av data i operasjonsrapporten for programmet inneholder data som lagres lokalt på datamaskinen og ikke sendes til Kaspersky.

Innsamling av data i henhold til lisensavtalen for sluttbrukere

Denne delen inneholder informasjon om spesifikk data som gis til Kaspersky hvis du har installert programversjonen som ikke er ment for bruk i EU, Storbritannia, Brasil eller av innbyggere i California.

Data for Kaspersky Basic

Data for Kaspersky Standard

Data for Kaspersky Plus- og Kaspersky Premium

Kaspersky beskytter den mottatte informasjonen i henhold til lovkrav og gjeldende regler for Kaspersky. Dataene overføres over krypterte kanaler.

For å forbedre sikkerhetsbevisstheten om nye trusler og deres kilder og for å forbedre sikkerhetsnivået ditt og produktets drift er rettighetshaveren, med ditt samtykke som eksplisitt er bekreftet i Kaspersky Security Network Data Collection Statement, uttrykkelig berettiget til å motta slik informasjon. Du kan deaktivere Kaspersky Security Network-tjenesten under installasjonen. Du kan også aktivere og deaktivere Kasperskys sikkerhetsnettverkstjeneste når som helst på Programvarens alternativside.

Du erkjenner og samtykker videre i at informasjonen som Rettighetshaveren har samlet inn, skal kunne bli brukt for å oppspore og publisere rapporter om sikkerhetsrisikotrender etter Rettighetshaverens eget og eksklusive skjønn.

Hvis du ikke ønsker at informasjonen som er samlet inn av programvaren, skal sendes til rettighetshaveren, bør du ikke aktivere og/eller deaktivere Kaspersky Security Network-tjenesten.

Innsamling av data i henhold til lisensavtalen for sluttbrukere på EUs territorium, Storbritannia, Brasil eller av innbyggere i California

Denne delen inneholder informasjon om spesifikk data som gis til Kaspersky hvis du har installert programversjonen som er ment for bruk i EU, Storbritannia, Brasil eller av inbyggere i California. **Informasjonen nevnt i denne delen inneholder ikke noe personlig data om brukeren og trengs for at rettighetshaverens programvare skal kunne kjøre, så fremt ikke noe annet spesifikk er oppgitt**.

Du sier deg enig i å, mens du bruker programmet, gi følgende data til Kaspersky for å forbedre kvaliteten til beskyttelsen i sanntid, forbedre kvaliteten til programvarens evne til å kjøre, og for å oppdage og rette feil i forbindelse med mekanismen for installering, fjerning og oppdatering av programvaren så raskt som mulig, antall brukere tatt i betraktning:

Data for Kaspersky Basic og Kaspersky Standard

Data for Kaspersky Plus- og Kaspersky Premium

For å forbedre kvaliteten på beskyttelsen av brukere som gjennomfører betalingstransaksjoner på nett, samtykker du i å automatisk gi det finansielle nettstedet informasjon om programvarens navn og versjon samt de egendefinerte innstillingene i programvaren, ID-en til programvarens tillegg i nettleseren som ble brukt til å åpne det finansielle nettstedet, ID-en som viser om en sikker eller vanlig nettleser ble brukt.

Informasjonen som mottas beskyttes av rettighetshaveren på måten som kreves av gjeldende lover, og er nødvendig for driften av programvaren som gjøres tilgjengelig for bruk under lisensen.

Kaspersky kan bruke statistikk innhentet basert på informasjonen som mottas, til å overvåke trender innen datasikkerhetstrusler, og til å publisere rapporter om slike trender.

Innlevering av data til Kaspersky Security Network

Hvilke data du sender til Kaspersky Security Network beskrives i erklæringen for Kaspersky Security Network.

Slik får du opp erklæringen for Kaspersky Security Network:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i programvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Gå til **Sikkerhetsinnstillinger** → **Kaspersky Security Network**.

   Vinduet **Kaspersky Security Network** åpnes med detaljer om Kaspersky Security Network og deltakelsesinnstillinger for Kaspersky Security Network.
4. Klikk på **Erklæring for Kaspersky Security Network** for å åpne teksten i erklæringen for Kaspersky Security Network.

Lagring av data i operasjonsrapporten for programmet

Rapportfiler kan inneholde personlige data som hentes inn under kjøring av beskyttelseskomponenter som Fil-Antivirus, E-post-Antivirus, Sikker surfing og Anti-Spam.

Rapportfiler kan inneholde følgende personlige data:

- IP-adressen til brukerens enhet
- Nettleserlogg
- Blokkerte koblinger
- Meldingslogg i sosiale nettverk
- Versjonen til nettleseren og operativsystemet
- Navn på informasjonskapsler og andre filer, samt banene til disse
- E-postadresser, avsendere, meldingsemner, meldingstekst, brukernavn og liste over kontakter

Når du bruker Beskyttelse for barn, Smart Home Monitor og komponenter for sikkerhetsnyheter, sender du følgende data

- Det trådløse nettverkets ID, det trådløse nettverkets status, enhets-ID, hash for enhetens MAC-adresse, enhetens status.
- Informasjon om besøkte nettsteder.
- Informasjon om antall ganger en fil har blitt startet på datamaskinen (filpopularitet).

Rapportfiler lagres lokalt på datamaskinen, og sendes ikke til Kaspersky. Bane til rapportfiler: %allusersprofile%\Kaspersky Lab\AVP21.7\Report\Database.

Rapporter lagres i følgende filer:

- reports.db
- reports.db-wal
- reports.db-shm (inneholder ikke personlige data)

Rapportfiler er beskyttet mot uautorisert tilgang hvis Selvforsvar er aktivert i Kaspersky. Hvis Selvforsvar er deaktivert, beskyttes ikke rapportfiler.

Lagre data for teknisk støtte

Programmet behandler og lagrer følgende personlige data slik at teknisk støtte kan analysere dem videre:

- Data som vises i programgrensesnittet:
  - E-postadressen som ble brukt ved tilkobling til My Kaspersky
  - Nettstedsadresser som ble lagt til unntakene (vist i komponentene Sikker surfing, Anti-Banner, Privat surfing og Nettverk, og i Rapporter-vinduet)
  - Lisensdata

  Disse dataene lagres lokalt i en ikke-endret form og kan vises under alle brukerkontoer på datamaskinen.
- Data i systemminnet til programprosesser i øyeblikket da en minnedump opprettes.
- Data som samles inn når sporing er aktivert.

Disse dataene lagres lokalt i en endret form og kan vises under alle brukerkontoer på datamaskinen. Disse dataene sendes til Kaspersky kun dersom du gir samtykke når du kontakte teknisk støtte. Hvis du vil vite mer om dataene, kan du klikke på lenken **Erklæring om teknisk støtte** i vinduet **Støtteverktøy**.

Om bruken av programvaren i EU, Storbritannia, Brasil eller av innbyggere i California

Versjonene av programmet som Kaspersky og våre partnere distribuerer i EU, Storbritannia, USA og Brasil (samt versjonene ment for bruk av innbyggere i California), oppfyller kravene i gjeldende forskrifter som regulerer innsamling og behandling av personopplysninger, i disse landene.

For å installere programmet må du godta lisensavtalen for sluttbrukere og vilkårene i personvernerklæringen.

I tillegg ber installasjonsveiviseren deg om å godta følgende avtaler om behandling av personopplysninger:

- Erklæring for Kaspersky Security Network. Denne erklæringen gir Kasperskys eksperter tillatelse til raskt å motta informasjon om trusler som oppdages på datamaskinen din, om programmer som kjøres, og signerte programmer som lastes ned, samt operativsysteminformasjon for å forbedre beskyttelsen.

- Erklæring angående databehandling til markedsføringsformål. Denne erklæringen gir oss tillatelse til å gi deg mer verdifulle tilbud.

- Erklæring om databehandling mens du bruker Anti-Spam. Denne erklæringen lar Kasperskys eksperter motta data for å forbedre komponenten Anti-Spam.

Du kan godta eller avslå Kaspersky Security Network-erklæringen og erklæringen om databehandling til markedsføringsformål når som helst fra vinduet **Innstillinger** → **Sikkerhetsinnstillinger** → **Kaspersky Security Network**.

Om Kaspersky-løsninger

De nye løsningene uttrykker visjonen vår om moderne nettsikkerhet. I tillegg til nye navn finner du et helt nytt brukergrensesnitt, og en rekke nye funksjoner.

Løsningene presenteres med flere planer. Planene varierer etter beskyttelsesnivå, og etter antall funksjoner og tjenester som gjøres tilgjengelig for brukere. Planene inneholder både nye og vel utprøvde funksjoner som faller innunder tre kategorier.

Utforsk funksjonene som er tilgjengelige for i hver kategori:

- Sikkerhet
- Ytelse
- Personvern

Sammenligning av abonnementsplaner

Programmet tilbyr fire abonnementsplaner. Tabellen nedenfor viser programfunksjonaliteten som er tilgjengelig for hver abonnementsplan.

Abonnementsplaner

Funksjon	Basic	Standard	Plus	Premium
My Kaspersky	✓	✓	✓	✓
Sikkerhet				
Hurtigskann	✓	✓	✓	✓
Fullstendig skann	✓	✓	✓	✓
Selektivt skann	✓	✓	✓	✓
Skanning av flyttbar stasjon	✓	✓	✓	✓
Bakgrunnsskan	✓	✓	✓	✓
Sårbarhetsskann	✓	✓	✓	✓
File Anti-Virus	✓	✓	✓	✓
Sikker surfing	✓	✓	✓	✓
E-post-Antivirus	✓	✓	✓	✓
Oppdatering av databaser og programmoduler	✓	✓	✓	✓
Rapporter	✓	✓	✓	✓
Karantene	✓	✓	✓	✓
Feilsøking av Microsoft Windows	✓	✓	✓	✓
Nødgjenoppretting	✓	✓	✓	✓
Utnyttelsesbeskyttelse	✓	✓	✓	✓
Systemvakt	✓	✓	✓	✓

Skann for svake innstillinger	✓	✓	✓	✓
Nettverkangrepsblokkering	✓	✓	✓	✓
URL-veileder	✓	✓	✓	✓
Utvidelse for Kaspersky Protection	✓	✓	✓	✓
Inntrengningsbeskyttelse		✓	✓	✓
Brannmur		✓	✓	✓
Nettverksovervåker		✓	✓	✓
Smart Home Monitor			✓	✓
Anti-Phishing		✓	✓	✓
Sikkerhetsnyheter		✓	✓	✓
Ytelse				
Rask oppstart		✓	✓	✓
PC Speed-Up		✓	✓	✓
Duplikater		✓	✓	✓
Store filer		✓	✓	✓
Ubrukte programmer		✓	✓	✓
Programoppdatering		✓	✓	✓
Gjeldende aktivitet		✓	✓	✓
Spillmodus		✓	✓	✓
Ikke forstyrr-modus		✓	✓	✓
Batterisparer		✓	✓	✓
Overvåking av harddiskens helse			✓	✓
Sikkerhetskopiering og gjenoppretting			✓	✓
Personvern				
Datalekkasjekontroll	enkelt konto	enkelt konto	✓	✓
Privat surfing		✓	✓	✓
Safe Money		✓	✓	✓
Webkamera og mikrofonkontroll		✓	✓	✓
Stalkerware-deteksjon		✓	✓	✓
Blokkering av installasjon av uønskede programmer		✓	✓	✓
Fjerning av annonseprogrammer		✓	✓	✓
Anti-Banner		✓	✓	✓
Personvernrengjøring		✓	✓	✓
Kaspersky VPN			✓	✓
Password Manager			✓	✓
Filmakulering			✓	✓

Hemmelig hvelv			✓	✓
Identitet				
Lommebok for identitetsbeskyttelse				✓
Deteksjon av fjerntilgang				✓
Premium-støttetjenester				✓

Maskinvare- og programvarekrav

Generelle krav

- 1500 MB ledig plass på harddisken
- Prosessor som støtter instruksjonssettet SSE2 (bortsett fra ARM)
- Internett-tilgang (for installasjon og aktivering av programmet, for bruk av Kaspersky Security Network og for oppdatering av databaser og programmoduler)
- Microsoft Windows® Installer 4.5 eller nyere
- Microsoft .NET Framework 4 eller nyere
- Microsoft .NET Desktop Runtime 5.x (5.0.10 eller høyere)
- Beskyttelse av tilgang til webkameraet er kun tilgjengelig for kompatible webkameramodeller

Krav til operativsystem

Operativsystem	CPU	Ledig RAM	Begrensninger
Microsoft Windows 11 Home (21H2, 22H2)	1 GHz eller høyere	4 GB (for et 64-biters operativsystem)	Windows Subsystem for Linux 2 (WSL2) støttes ikke.
Microsoft Windows 11 Enterprise (21H2, 22H2)			
Microsoft Windows 11 Pro (21H2, 22H2)			
Microsoft Windows 10 Home (versjoner: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)	1 GHz eller høyere	1 GB (for 32-biters operativsystemer) eller 2 GB (for 64-biters operativsystemer)	
Microsoft Windows 10 Enterprise (versjoner: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)			
Microsoft Windows 10 Pro (versjoner: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)			
Microsoft Windows 8.1 (Service Pack 0 eller nyere, Windows 8.1 Update)	1 GHz eller høyere	1 GB (for 32-biters operativsystemer) eller 2 GB (for 64-biters operativsystemer)	
Microsoft Windows 8.1 Pro (Service Pack 0 eller nyere, Windows 8.1 Update)			

Microsoft Windows 8.1 Enterprise (Service Pack 0 eller nyere, Windows 8.1 Update)			
Microsoft Windows 8 (Service Pack 0 eller nyere)	1 GHz eller høyere	1 GB (for 32-biters operativsystemer) eller 2 GB (for 64-biters operativsystemer)	
Microsoft Windows 8 Pro (Service Pack 0 eller nyere)			
Microsoft Windows 8 Enterprise (Service Pack 0 eller nyere)			
Microsoft Windows 7 Starter (Service Pack 0 eller nyere)	1 GHz eller høyere	1 GB (for 32-biters operativsystemer) eller 2 GB (for 64-biters operativsystemer)	
Microsoft Windows 7 Home Basic (Service Pack 0 eller nyere)			
Microsoft Windows 7 Home Premium (Service Pack 0 eller nyere)			
Microsoft Windows 7 Professional (Service Pack 0 eller nyere)			
Microsoft Windows 7 Ultimate (Service Pack 0 eller nyere)			

Beskyttelseskomponentene Sikker surfing, Anti-Banner og Safe Money krever at tjenesten Base Filtering Engine er aktivert i operativsystemet.

Støtte for nettlesere

Følgende nettlesere støtter installasjon av utvidelsen for Kaspersky Protection:

- Chromium-basert Microsoft Edge 77.x – 104.x;
- Mozilla™ Firefox™-versjoner 52.x – 105.x;
- Mozilla™ Firefox™ ESR 52.x, 60.x, 68.x, 78.x, 91.x; 102.x;
- Google Chrome™-versjoner 48.x – 105.x.

Følgende nettlesere støtter Skjermtastatur og skanning av krypterte tilkoblinger:

- Chromium-basert Microsoft Edge 77.x – 104.x;
- Mozilla Firefox-versjoner 52.x – 105.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x; 102.x;
- Google Chrome 48.x – 105.x.

Følgende nettlesere støtter modusen Beskyttet nettleser:

- Microsoft Internet Explorer 11.0;
- Chromium-basert Microsoft Edge 77.x – 104.x;

- Mozilla Firefox-versjoner 52.x – 105.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x, 102.x;
- Google Chrome 48.x – 105.x;
- Yandex Browser 18.3.1 – 22.9.1 (med begrensninger).

Nyere versjoner av nettlesere kan støttes hvis nettleseren støtter den aktuelle teknologien.

Kaspersky støtter Google Chrome og Mozilla Firefox både i 32-biters og i 64-biters operativsystemer.

Krav for nettbrett

- Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10, Microsoft Windows 11;
- Intel® Celeron®-prosessor med en klokkehastighet på 1,66 GHz eller høyere;
- 1000 MB ledig RAM.

Krav for nett-PCer

- Intel Atom™ CPU 1.60 GHz eller raskere
- 1024 MB ledig RAM
- 10,1-tommers skjerm med 1024x768 skjermoppløsning
- Intel GMA 950 grafikkprosessor eller nyere

Kravene for Kaspersky Password Manager er tilgjengelige i hjelpefilene for programmet.

Kompatibilitet med andre Kaspersky-programmer

Kaspersky er kompatibelt med følgende Kaspersky-programmer:

- Kaspersky Safe Kids 1.5
- Kaspersky Password Manager 10
- Kaspersky Software Updater 2.1
- Kaspersky Virus Removal Tool 2015, 2020
- Kaspersky VPN Secure Connection 4.0, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8.

Dette er nytt i den nyeste versjonen av programmet

Den nyeste versjonen av programmet innfører følgende nye funksjoner og forbedringer:

- Lydstrøm Beskyttelse Funksjonaliteten kalles nå Mikrofonkontroll og kan finnes under Webkamera og mikrofonkontroll i Personvern-delen.

- Devices on My Network-funksjonaliteten kalles nå Smart Home Monitor. Listen over enhetstyper som kan legges til av brukeren er utvidet.

- I Kaspersky Premium:

  - Beskyttelsen når du kobler til Wi-Fi-nettverk er forbedret. Programmet oppdager nå Wi-Fi-nettverksinnstillinger som ikke er sikre nok.

  - Funksjonalitet for å oppdage fjerntilgangsprogrammer på datamaskinen din er lagt til.

- Et nytt vindu viser en forklaring på hvordan automatisk fornyelse fungerer.

- Scenarioet for å bytte til Kaspersky-programmet på andre plattformer er forbedret. Linken tar deg ikke lenger til My Kaspersky; det åpner et vindu direkte for nedlasting av programmet på en annen plattform.

- Rettet feilen der WPA3-protokollen ble oppdaget som usikker.

- Varslinger knyttet til behovet for en omstart av datamaskinen er forbedret.

Slik fungerer abonnementet

Slik fungerer betalte abonnementer

Abonnementet fornyes automatisk ved slutten av hver periode, med mindre du sier det opp. Mot slutten av den betalte perioden mottar du en e-post med en påminnelse om den kommende belastningen. Betalingen for neste periode skjer før den gjeldende perioden utløper, for å sikre at du får uavbrutt beskyttelse mot sikkerhetstrusler på nett. Hvis abonnementet fornyes, legges de resterende dagene for den inneværende perioden til i den nye perioden.

Vær oppmerksom på at prisen på abonnementet kan variere. Når du fornyer kan det hende at det finnes spesialtilbud og rabatter som ikke påvirker abonnementet ditt.

Slik fungerer gratis abonnementer

Det gratis prøveabonnementet blir aktivt med en gang du begynner å abonnere. Noen dager før prøveperioden utløper vil du motta en påminnelse om fornyelse av abonnement. Hvis du ikke sier opp abonnementet i løpet av prøveperioden, fornyes abonnementet automatisk for neste periode så snart prøveperioden utløper.

Hvis det oppstår et problem med betalingen

Hvis abonnementet ditt av en eller annen grunn ikke kan fornyes automatisk (bankkortet ditt er utløpt, er blitt blokkert eller automatisk fornyelse er deaktivert), kan du få en respittperiode for å fornye abonnementet når det utløper. Du kan bruke alle funksjoner i programmet uten begrensninger mens respittperioden er aktiv. Hvis du ikke har fornyet abonnementet når respittperioden utløper, bytter programmet eventuelt til modus for begrenset funksjonalitet. Varigheten til begrenset funksjonalitetsmodus vil variere avhengig av regionen din og av lisensvilkårene. Se delen Profil for informasjon om utløpsdatoen for respittperioden og begrenset funksjonalitet.

Om abonnementer kjøpt av tjenesteleverandører

Du kan abonnere gjennom en tjenesteleverandør (for eksempel Internett-leverandøren din). Du kan avbryte og gjenoppta abonnementet, fornye det automatisk eller annullere det. Du kan administrere abonnementet ved å gå til kontoen din på nettstedet til tjenesteleverandøren du abonnerte gjennom. Avhengig av tjenesteleverandøren kan alternativene for behandling av abonnementet variere.

Bruk aktiveringskoden du fikk av tjenesteleverandøren for å aktivere abonnementet på enheten din. I enkelte tilfeller kan aktiveringskoden lastes ned og brukes automatisk.

Hvis et annet abonnement allerede er aktivt i programmet når du abonnerer gjennom en tjenesteleverandør, brukes programmet med abonnementet fra tjenesteleverandøren. Det gjeldende abonnementet kan brukes på en annen enhet til det utløper.

Et abonnement kan være ubegrenset (uten utløpsdato) eller begrenset (for eksempel til ett år). Ubegrensede abonnementer fornyes automatisk så lenge tjenesteleverandøren har mottatt forhåndsbetaling til rett tid. Hvis du vil fortsette å bruke programmet når abonnementet har utløpt, må du fornye det selv.

Når du bruker programmet med et abonnement du skaffet gjennom en tjenesteleverandør, kan du ikke legge til en reserve-aktiveringskode for å holde abonnementet i gang.

Hvis du ikke fornyet abonnementet, eller tjenesteleverandøren ikke kunne fornye abonnementet automatisk, kan det hende du får en frist for å fornye abonnementet når det utløper. Programmets funksjoner forblir tilgjengelige i respittperioden. Programmet kan bytte til modus for begrenset funksjonalitet når fristen utløper. Hvis tjenesteleverandøren ikke tilbyr en respittperiode eller modus for begrenset funksjonalitet, vil ingen av programmets funksjoner være tilgjengelige når abonnementet utløper.

Om abonnementer kjøpt gjennom App Store, Google Play eller Huawei AppGallery

Hvis du har kjøpt et abonnement gjennom App Store, Google Play eller Huawei AppGallery, kan du se abonnementsdetaljene i den aktuelle appbutikken.

Slik kjøper du et abonnement

Det er flere måter å skaffe seg et abonnement på et program på:

Kjøp på Kasperskys nettsted

Du kan kjøpe et abonnement på programmet på Kasperskys nettsted:

Kjøp Kaspersky Basic

Kjøp Kaspersky Standard

Kjøp Kaspersky Plus

Kjøp Kaspersky Premium

Kaspersky Premium er ikke tilgjengelig i enkelte regioner.

Kjøp ved hjelp av programgrensesnittet

Slik kjøper du et abonnement i programgrensesnittet:

1. Åpne hovedvinduet.
2. Gå til delen **Profil**. Hvis enheten din er koblet til My Kaspersky-kontoen din, vises e-postadressen din her.
3. Klikk på **Kjøp nå** i abonnementsinformasjonen.

   Nettstedet til Kaspersky eller en av våre partnere åpnes i standardnettleseren. Følg instruksjonene på nettstedet.

Kjøp fra en Kaspersky-partner

Du kan kjøpe et abonnement i butikken til en Kaspersky-partner.

Slik administrerer du abonnementet fra My Kaspersky-kontoen din

Du trenger en *My Kaspersky-konto* for å bruke programmet.

Avhengig av abonnementet ditt, kan det være nødvendig å koble enheten du installerer programmet på til My Kaspersky-kontoen din for å få tilgang til noen eller alle programfunksjoner.

I My Kaspersky-kontoen kan du:

- vise informasjon om abonnementer og når de utløper
- fjernstyre beskyttelsen av enheten
- sikkert lagre og synkronisere passordene dine og andre personopplysninger hvis du bruker Kaspersky Password Manager
- laste ned programmer du har kjøpt
- kontakte teknisk støtte
- lese mer om nye programmer og spesialtilbud fra Kaspersky

Se hjelpedelen for My Kaspersky for detaljer om all funksjonalitet for My Kaspersky-kontoen.

Slik kobler du en enhet til My Kaspersky-kontoen

Hvis du kjøpte abonnementet fra Kasperskys nettsted, ble det opprettet en konto under kjøpsprosessen. En e-post med koblingen for oppretting av passord ble sendt til e-postadressen du oppga under kjøpet.

Du kan logge på My Kaspersky-kontoen ved å angi e-postadresse og passord, eller ved å bruke Google-, Facebook- eller Apple-kontoen din. Hvis du allerede har en konto, kan du konfigurere rask pålogging med Google-, Facebook- eller Apple-kontoen din i vinduet som brukes til å koble enheten til My Kaspersky-kontoen din. Dette kan skje hvis du brukte e-postadressen fra Google-, Facebook- eller Apple-kontoen din da du opprettet My Kaspersky-kontoen din.

Pålogging med Facebook og Google er ikke tilgjengelig i noen områder.

Hvis du ikke har en konto enda, kan du opprette en i prosessen for å koble enheten til kontoen din. Du kan også logge på kontoen din med påloggingsdetaljer fra andre Kaspersky-ressurser.

Slik kobler du enheten din til My Kaspersky-kontoen:

1. Du kan koble en enhet til kontoen din:
   - i tilkoblingsvinduet når du aktiverer programmet
   - i brukergrensesnittet for programmet, i delen **Profil**.

     I blokken **Logg på My Kaspersky** klikker du på **Logg på**-knappen.
   - på My Kasperskys nettsted
   - når du aktiverer visse funksjoner i programmet
2. I vinduet for tilkobling av kontoen velger du tilkoblingsmetoden du synes er mest praktisk:
   - **Logg på med en e-postadresse**. Skriv inn e-postadressen din i tekstboksen. En melding med en kobling for oppretting av passord sendes til den angitte e-postadressen.

     Hvis du har konfigurert totrinnsverifisering for My Kaspersky-kontoen din, sendes en tekstmelding med verifiseringskoden til telefonen din. Skriv inn verifiseringskoden i feltet og klikk på **Fortsett**.
   - **Logg på med Google-, Facebook- eller Apple-konto**.

     a. Klikk **Logg på med Google**, **Logg på med Facebook** eller **Logg på med Apple**.

     Dette åpner et nettleservindu. I dette vinduet kan du logge på Google-, Facebook- eller Apple-kontoen din og gi programmet tilgang til e-postadressen din.

     Hvis du ikke har en Google-, Facebook- eller Apple-konto, kan du opprette en og fortsette med å konfigurere task pålogging til My Kaspersky.

     Hvis totrinnsverifisering er konfigurert for My Kaspersky-kontoen din, konfigurerer du rask pålogging for kontoen din på My Kaspersky-nettstedet, går tilbake til programmet og logger på med Google, Facebook eller Apple.

     Hvis du bruker Microsoft Edge til å konfigurere påloggingen til My Kaspersky, trenger du en versjon av Microsoft Edge basert på Chromium 77.x eller nyere. Hvis det oppstår en tilkoblingsfeil, velger du en annen nettleser som standard nettleser, installerer den nyeste versjonen av Microsoft Edge-nettleseren eller oppdater Microsoft Windows-operativsystemet.

     b. Gå tilbake til programmet og fortsett med å opprette kontoen ved å klikke på **Fortsett**. Følg instruksjonene som vises på skjermen.

     Enheten din blir vil bli tilkoblet til My Kaspersky-kontoen din. I tillegg kan du sette opp et passord for kontoen din på My Kaspersky-nettstedet.

     Databehandling når du logger på kontoen

Følgende data behandles når du logger på My Kaspersky-kontoen med Google, Facebook eller Apple:

- Rettighetshaverens ressurs-ID
- Verdi generert for verifisering av forespørsel
- Tokentype
- URI som svaret fra godkjenningsleverandøren sendes til

Følgende data behandles når du logger på kontoen på nettstedet til en tjenesteleverandør ved hjelp av godkjenningsleverandører:

- Rettighetshaverens ressurs-ID
- Token brukt til godkjenning i tjenesteleverandørens infrastruktur
- Tokentype
- Parametere forespurt fra godkjenningsleverandørene
- URI som svaret fra godkjenningsleverandøren sendes til

I noen områder ber programmet deg om å lese og godta erklæringen om databehandling for bruk av nettportalen. Hvis du godtar vilkårene i erklæringen, klikker du på **Godta**.

Slik sier du opp abonnementet

Du kan si opp abonnementet når som helst. Et oppsagt abonnement fornyes ikke automatisk, og enhetene dine forblir beskyttet frem til den siste betalte perioden utløper.

Hvis du vil unngå unødvendige utgifter, bør du si opp abonnementet ditt før betalingsdatoen for neste periode. Vær oppmerksom på at betalingen skjer før den nåværende perioden utløper, for å sikre at beskyttelsen opprettholdes uten avbrudd.

Slik sier du opp abonnementet i Russland, Hviterussland, Abkhasia, Armenia, Aserbajdsjan, Georgia, Sør-Ossetia, Kirgisistan, Mongolia, Tadsjikistan, Turkmenistan, Usbekistan, Kasakhstan

Slik sier du opp abonnementet:

1. Sjekk innboksen for e-postadressen du oppga da du foretok kjøpet. I e-posten med bestillingsbekreftelse eller påminnelse om fornyelse av abonnementet finner du en kobling til kontoen din, eller en kobling til siden for administrering av automatisk fornyelse.
2. Klikk på koblingen.

   I standardnettleseren tas du til den personlige siden din på betalingsleverandørens nettsted.
3. Du kan si opp abonnementet på siden med informasjon om fornyelse.

   Abonnementet er sagt opp. En e-post med bekreftelse på oppsigelsen sendes til e-postadressen din.

Slik sier du opp abonnementet i andre land

Slik sier du opp abonnementet:

1. Åpne hovedvinduet.
2. Gå til delen **Profil**.
3. Klikk på **Administrer konto** i abonnementsinformasjonen. Hvis du ikke koblet enheten til kontoen din, klikker du på **Logg på**.

   Vinduet for å logge på My Kaspersky-kontoen åpnes.
4. Gå til **Abonnementer** i My Kaspersky-kontoen din og klikk på abonnementspanelet.

   Et vindu med abonnementsdetaljer åpnes.
5. Klikk på **Administrer abonnement**.

   Velg **Si opp abonnementet** i rullegardinlisten. Følg instruksjonene på skjermen.

Abonnementet er sagt opp.

Hvis du sier opp abonnementet etter den automatiske betalingen for neste periode, forblir abonnementet aktivt til neste periode utløper. Hvis du ønsker å kansellere betalingen for perioden som allerede har gått gjennom, kan du be om refusjon i henhold til retningslinjene for refusjon. Vanligvis kan du få refusjon innen 30 dager etter betalingen. Kontakt teknisk støtte for mer informasjon om betingelser og tilgjengeligheten av refusjon.

Når du ber om refusjon, må du oppgi følgende informasjon:

- Kjøpsdato
- Navnet og e-postadressen du oppga da du gjennomførte kjøpet
- Bestillingsnummer

Etter at du har bekreftet informasjonen du oppga, tar det mellom fem og sju virkedager før du mottar pengene.

Slik angir du en annen betalingsmetode

Automatisk belastning for fornyelse av abonnement bruker betalingsmetoden du valgte da du kjøpte abonnementet. Du kan angi en annen betalingsmetode.

Slik angir du en annen betalingsmetode i Russland, Hviterussland, Abkhasia, Armenia, Aserbajdsjan, Georgia, Sør-Ossetia, Kirgisistan, Mongolia, Tadsjikistan, Turkmenistan, Usbekistan, Kasakhstan

Slik angir du en annen betalingsmetode:

1. Sjekk innboksen for e-postadressen du oppga da du foretok kjøpet. I e-posten med bestillingsbekreftelse eller påminnelse om fornyelse av abonnementet finner du en kobling til kontoen din, eller en kobling til siden for administrering av automatisk fornyelse.
2. Klikk på koblingen.

   I standardnettleseren tas du til den personlige siden din på betalingsleverandørens nettsted.
3. På siden med informasjon om fornyelse av abonnement, endrer du betalingsmetode og lagrer endringene.

Slik angir du en annen betalingsmetode i andre land

Slik angir du en annen betalingsmetode:

1. Åpne hovedvinduet.
2. Gå til delen **Profil**.
3. Klikk på **Administrer konto** i abonnementsinformasjonen. Hvis du ikke koblet enheten til kontoen din, klikker du på **Logg på**.

   Dette åpner påloggingsvinduet for My Kaspersky i den standard nettleseren.
4. Klikk på koblingen med e-postadressen øverst til høyre på siden.
5. Velg **Kontoinnstillinger** i rullegardinlisten.
6. Klikk på fanen **Betalingsmetode**.
7. Klikk på  .

   Velg **Rediger** i rullegardinmenyen.
8. Du tas til redigeringssiden for betalingsmetoder på nettstedet til vår offisielle Nexway i et nytt nettleservindu. Følg instruksjonene på skjermen for å angi en annen betalingsmetode.

Slik aktiverer du et abonnement på enheten din

I denne delen lærer du hvordan du begynner å bruke programmer etter at du har kjøpt et abonnement. Du må ha Internett-tilkobling for å aktivere.

Hvis du har kjøpt et abonnement på Kasperskys nettsted

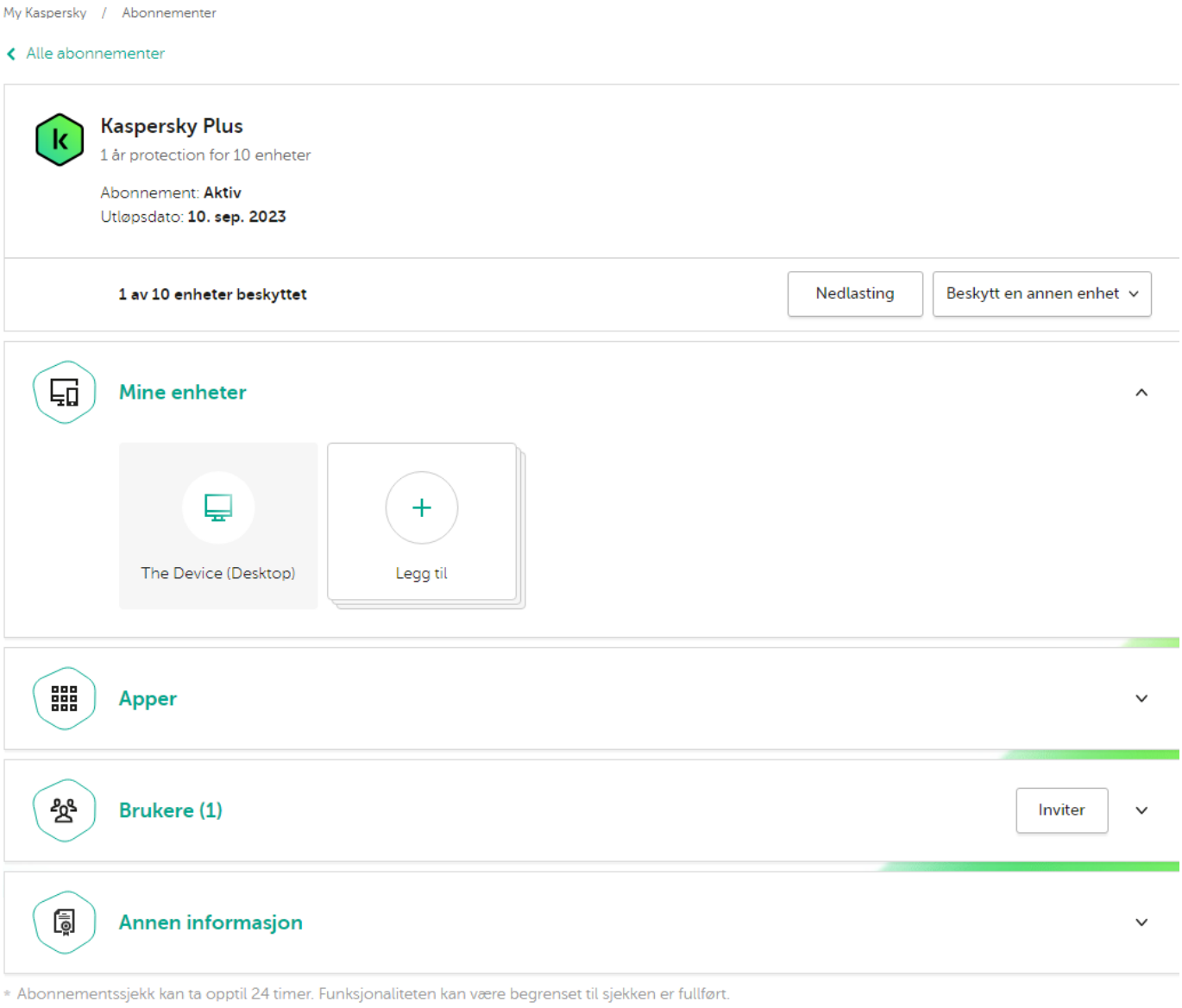
Hvis du kjøpte abonnementet i Kasperskys nettbutikk, ble My Kaspersky-kontoen din opprettet i løpet av kjøpet. Du må ha en My Kaspersky-konto for å aktivere abonnementet på forskjellige enheter og administrere abonnementet det. Du kan aktivere abonnementet ditt ved å logge på My Kaspersky-kontoen fra enheten du installerer programmet på.

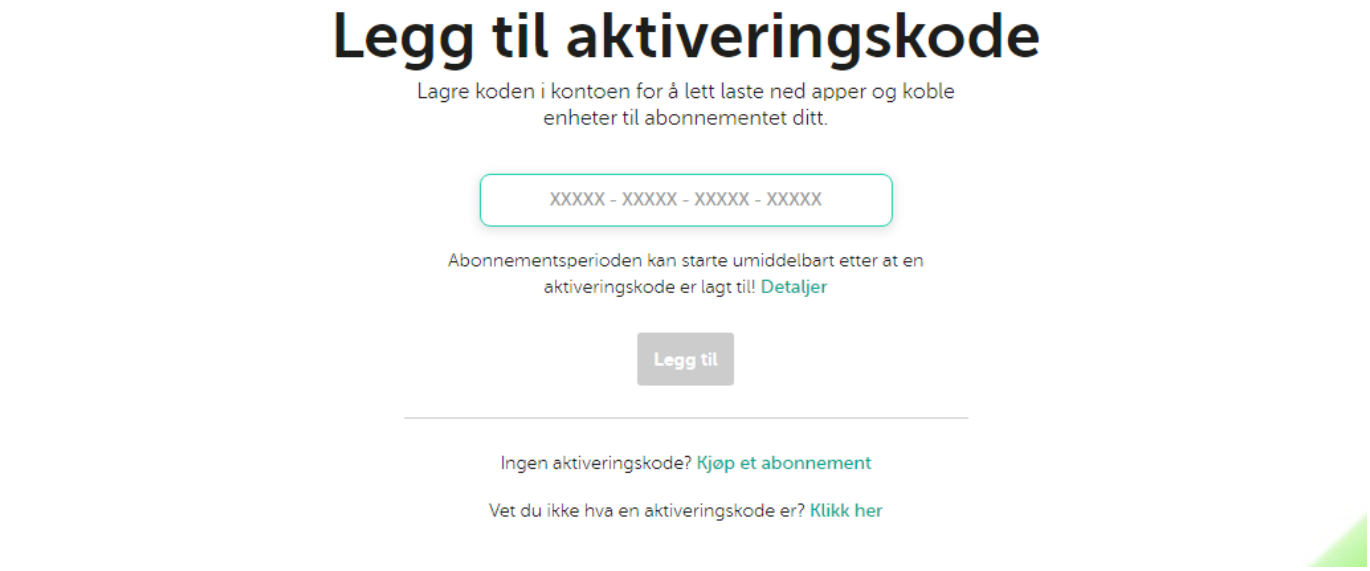
Slik aktiverer du et abonnement på enhetene dine:

1. Sjekk innboksen for e-postadressen du oppga da du foretok kjøpet. Du skal ha mottatt to e-poster fra Kaspersky: en med kvittering og en med instruksjoner for å fullføre aktiveringen av abonnementet.

2. Klikk på **Gå til My Kaspersky** i e-posten med instruksjoner for å fullføre opprettelsen av kontoen din og logge på.

3. Klikk på **Last ned** i vinduet med abonnementsinformasjon for å laste ned programmet på enheten din.





4. Installer programmet.

Når installasjonen er fullført, kobles programmet automatisk til kontoen din og aktiveres med abonnementet du har kjøpt.

Når et abonnement fornyes, oppdateres utløpsdatoen automatisk innen 24 timer på alle enhetene som er aktivert for dette abonnementet og koblet til My Kaspersky-kontoen din.

Hvis du kjøper et abonnement fra Kasperskys nettbutikk, begynner abonnementsperioden fra øyeblikket du gjennomfører kjøpet.

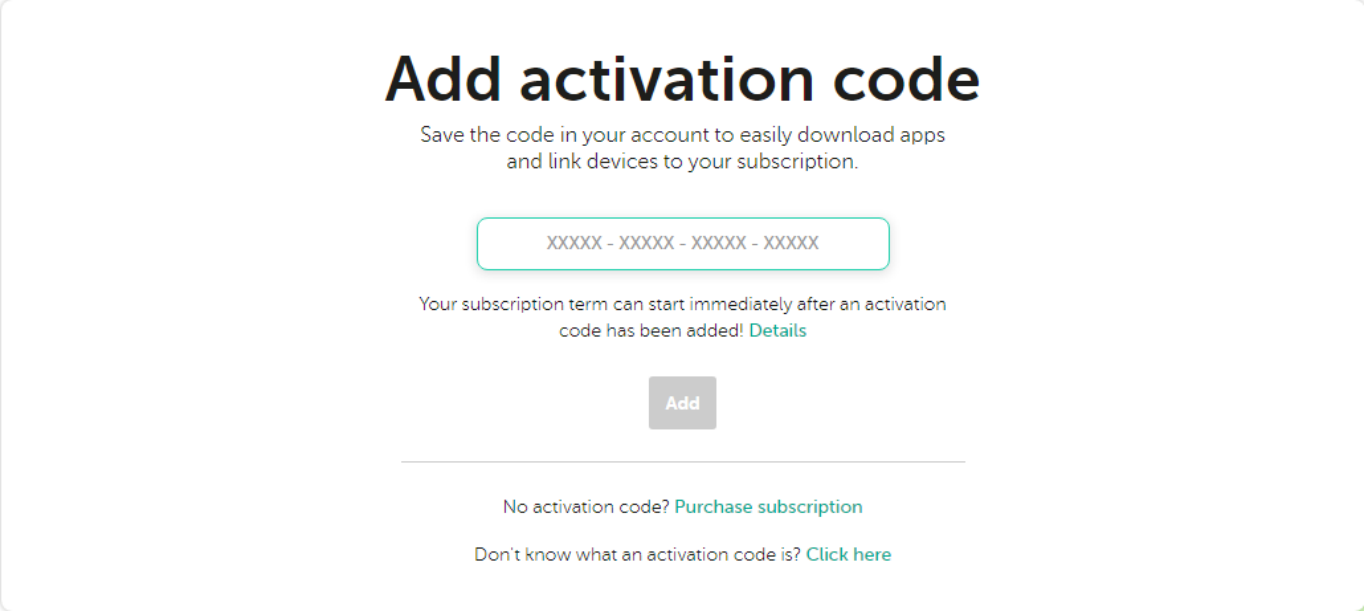
Hvis du har kjøpt en boks eller et aktiveringskort

Hvis du har kjøpt en boks eller et aktiveringskort i en butikk, trenger du en aktiveringskode for å aktivere programmet. Du finner aktiveringskoden på boksen, i dokumentasjonen eller på baksiden av kortet. Aktiveringskoden er en unik sekvens med 20 sifre og latinske bokstaver i formatet xxxxx-xxxxx-xxxxx-xxxxx.

Nedtellingen for utløp av et abonnement som er aktivert med en aktiveringskode starter fra datoen du aktiverer programmet på den første enheten.

Hvis du har kjøpt et aktiveringskort:

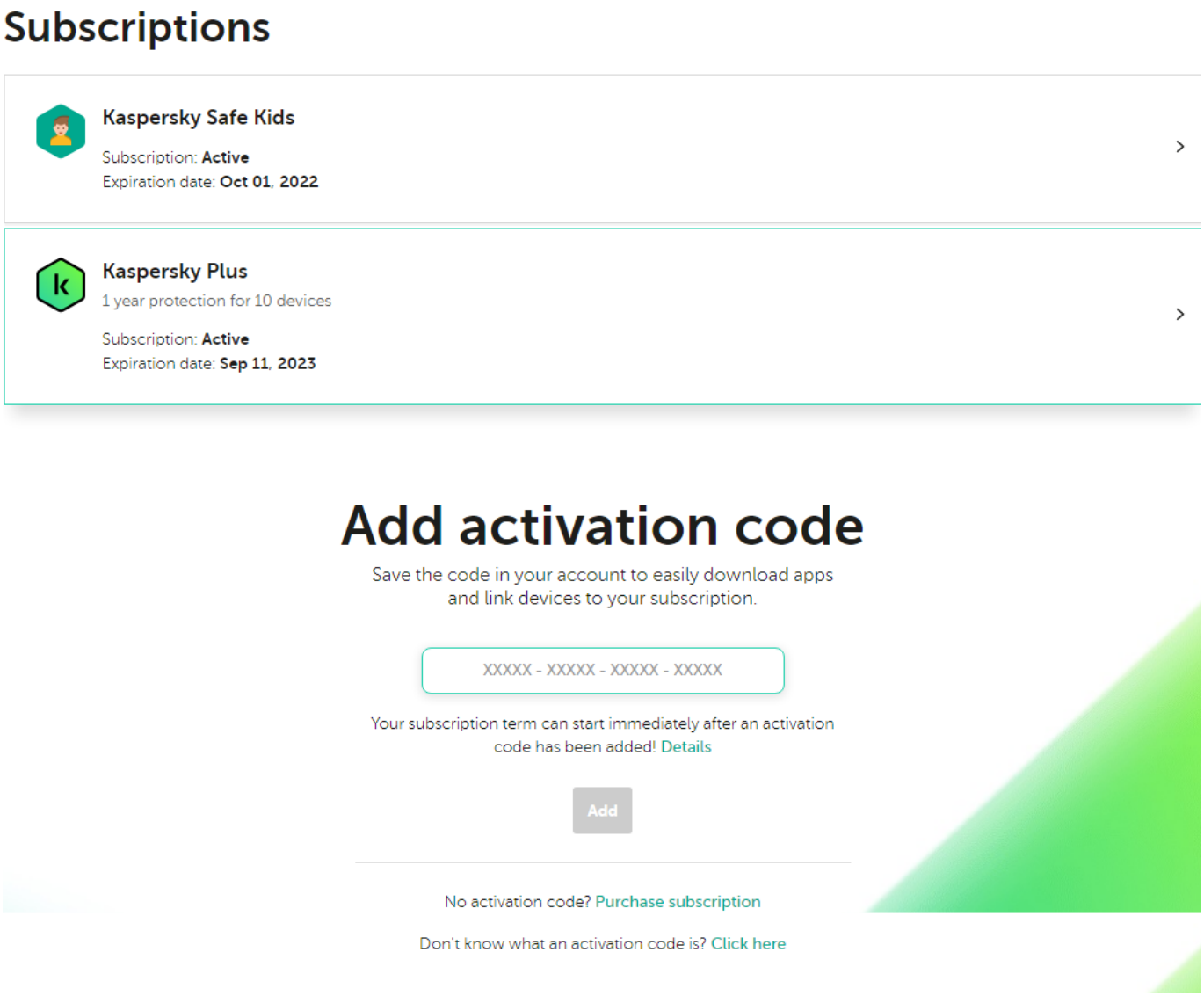
1. Åpne My Kasperskys nettsted på enheten du vil beskytte.
2. Opprett en My Kaspersky-konto eller logg på en eksisterende konto.
3. Under **Har du allerede en aktiveringskode?** i den nedre delen av siden, skriver du inn aktiveringskoden i registreringsfeltet.



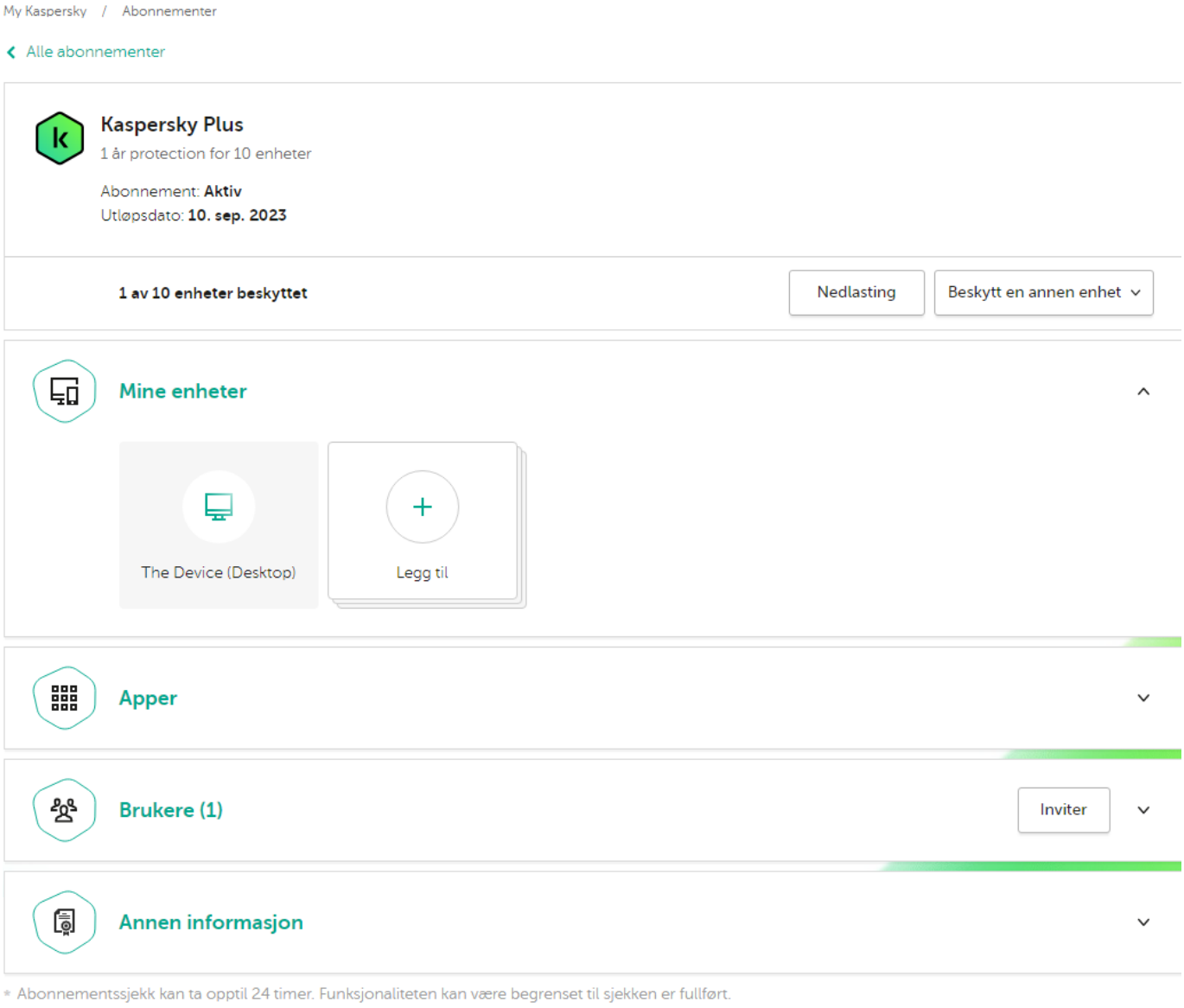
4. Klikk på **Legg til**.

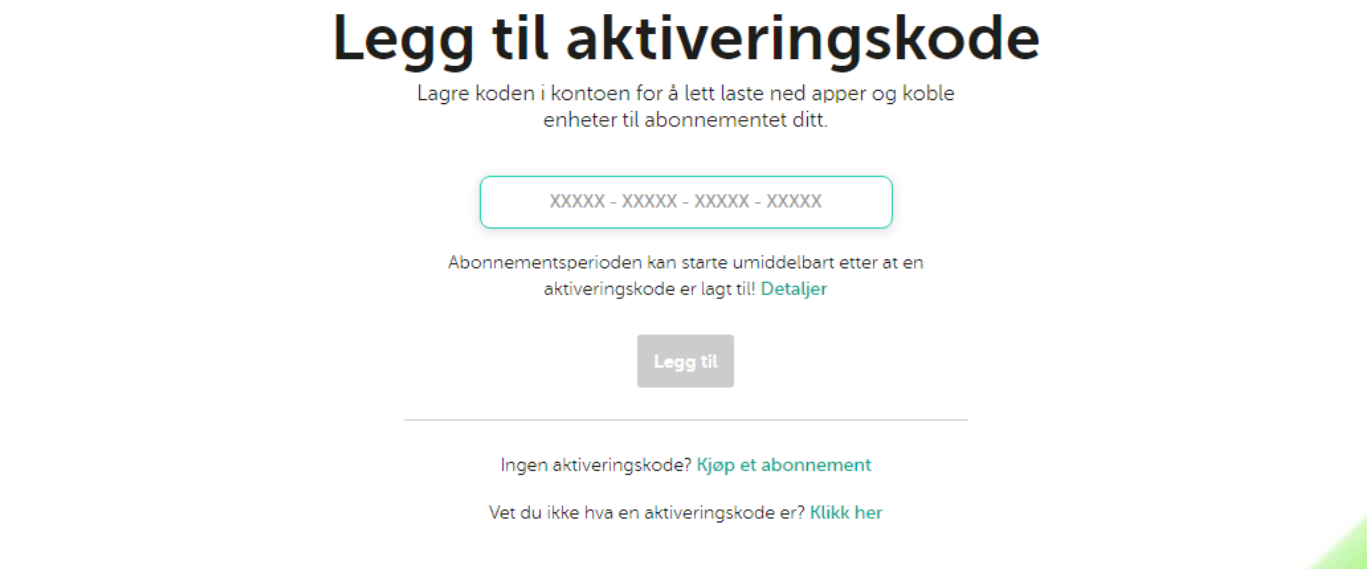
   Hvis aktiveringskoden ble lagt til, viser delen **Abonnementer** abonnementspanelet.

5. Klikk på abonnementspanelet.



6. Klikk på **Last ned** i vinduet med abonnementsinformasjon for å laste ned programmet på enheten din.





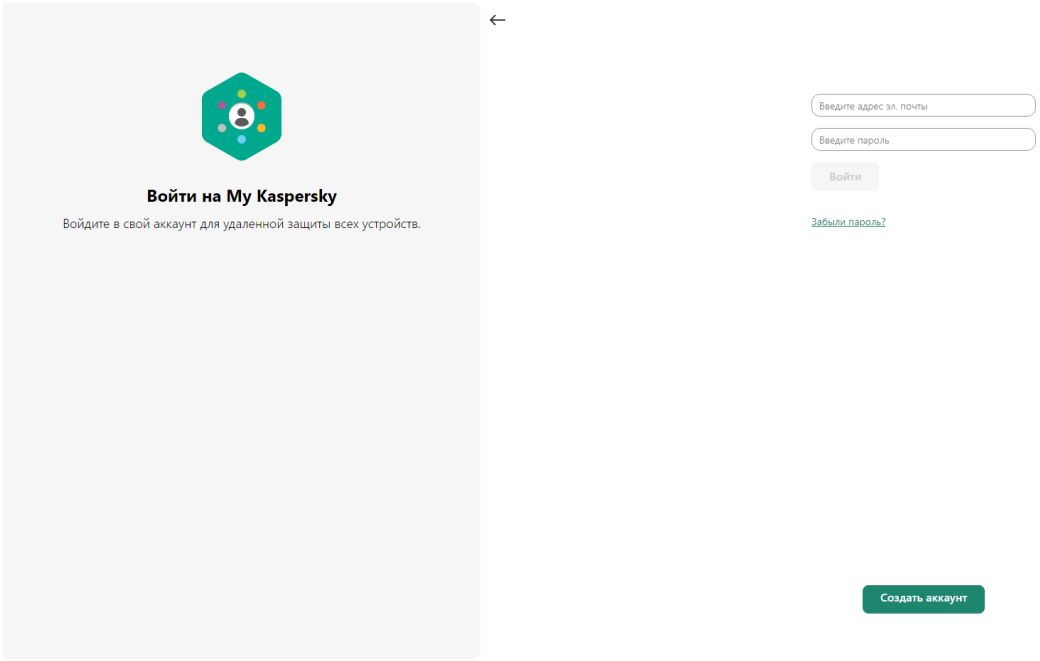
7. Installer programmet.

   Etter at programmet er ferdig installert, aktiveres den automatisk i henhold til vilkårene for abonnementet ditt.

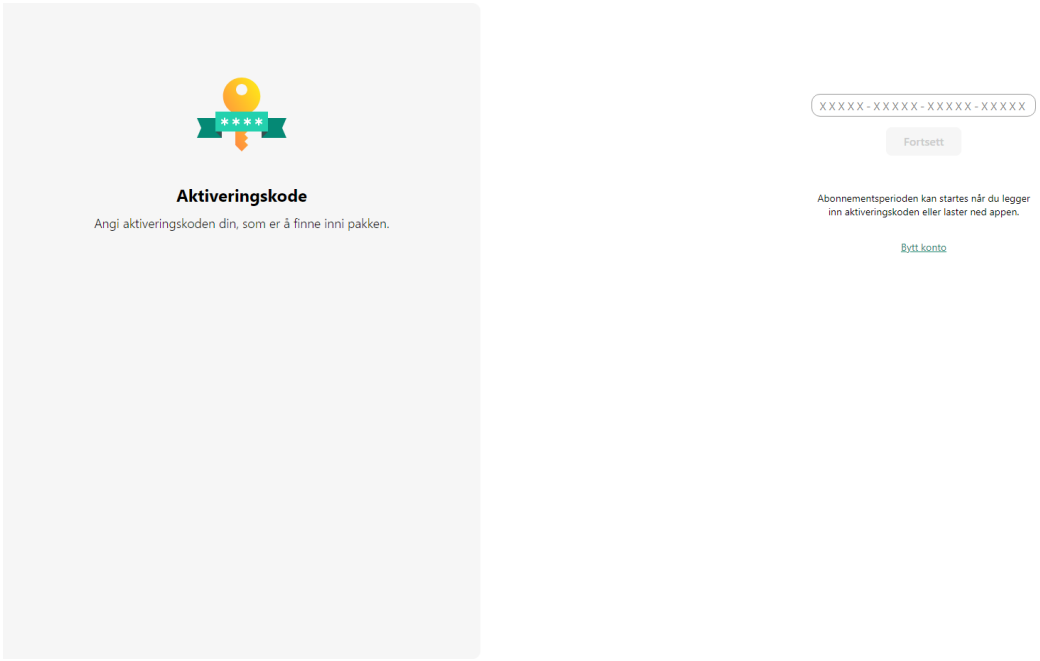
Hvis du har kjøpt en boks med en installasjonsdisk:

1. Sett inn disken i diskstasjonen.

2. I vinduet for å koble kontoer til My Kaspersky, oppretter du en konto eller logger på en eksisterende konto.

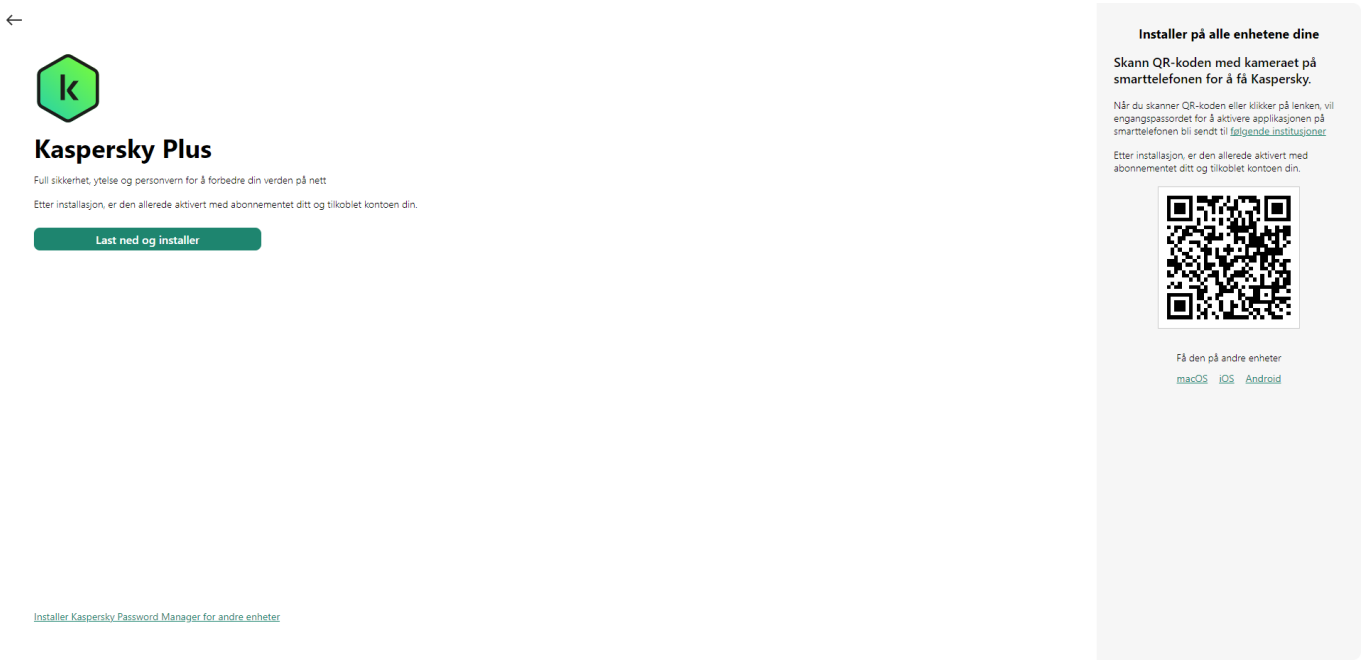


3. I vinduet for aktivering av aktiveringskode skriver du inn aktiveringskoden i tekstboksen og klikker på **Fortsett**.



Aktiveringskoden er lagret på kontoen din under **Abonnementer**.

4. Klikk på **Last ned og installer** for å laste ned og installere programmet på enheten din.



5. Installer programmet.

   Etter at programmet er ferdig installert, aktiveres den automatisk i henhold til vilkårene for abonnementet ditt.

Aktiveringskoden er nå lagret på My Kaspersky-kontoen din. Hvis du vil beskytte en ny enhet, logger du på kontoen din og laster ned programmet. Du kan også angi aktiveringskode manuelt i programmet.

Aktivere abonnementet hvis programmet allerede er installert på enheten din

I denne delen lærer du hvordan du fornyer et utløpt abonnement, legger til en ny aktiveringskode for et program som har et aktivt abonnement for å få det fornyet automatisk, og bytter fra prøveabonnementet til et betalt abonnement.

Abonnementet har utløpt

Hvis du har aktivert automatisk fornyelse, fornyes abonnementet automatisk for en ny periode, uten at du trenger å gjøre noe. Hvis du ikke har aktivert automatisk fornyelse, må du fornye abonnementet manuelt.

Hvis du fornyer abonnementet manuelt, og du har lagt til en reserve-aktiveringskode i programmet tidligere, aktiveres programmet automatisk med reserve-aktiveringskoden når det gjeldende abonnement utløper.

Slik fornyer du et abonnement:

1. Åpne hovedvinduet.
2. Gå til delen **Profil**. Hvis enheten din er koblet til My Kaspersky-kontoen din, vises e-postadressen din her.
3. Klikk på **Forny nå** i abonnementsinformasjonen.

   Nettstedet til Kaspersky eStore eller en av våre partnere åpnes i standardnettleseren.

Under kjøpsprosessen skriver du inn e-postadressen som er registrert for My Kaspersky-kontoen din. Hvis du ikke har en konto enda, vil den bli opprettet med den angitte e-postadressen. Etter at du har kjøpt programmet og koblet det til My Kaspersky-kontoen din, aktiveres abonnementet automatisk på enheten innen en time etter fornyelse.

Du kan også sende det nye abonnementet til enheter fra My Kaspersky-kontoen din. Se hjelpedelen for My Kaspersky for informasjon om hvordan du sender et abonnement til en enhet som er koblet til kontoen din.

Hvis du ikke har fornyet abonnementet, kan det hende at programmet bytter til modus for begrenset funksjonalitet.

Fornye abonnementet med en reserve-aktiveringskode

Hvis du har en ny aktiveringskode, kan du legge den til i programmet for å bruke den som reservekode. Når det gjeldende abonnementet utløper, aktiveres programmet automatisk med reserve-aktiveringskoden. På denne måten kan du sikre uavbrutt beskyttelse for enheten din.

Det finnes tilfeller der **du ikke kan** legge til en reserve-aktiveringskode.

Det kan hende du ikke kan legge til en reserve-aktiveringskode kan være utilgjengelig på grunn av følgende begrensninger:

- Du kan ikke legge til en reserve-aktiveringskode hvis du bruker et automatisk fornyet abonnement.
- En aktiveringskode for et abonnement med automatisk fornyelse kan ikke legges til som en reserve-aktiveringskode.
- Du kan ikke legge til en reserve-aktiveringskode hvis du bruker et prøveabonnement.
- En aktiveringskode er allerede angitt i programmet som reserve-aktiveringskode.
- Du kan ikke legge til en reservekode hvis gjeldende abonnement allerede er utløpt.
- Abonnementet er ikke tilgjengelig i regionen din enda.

Slik legger du til en reserve-aktiveringskode:

1. Åpne hovedvinduet.
2. Gå til delen **Profil**. Hvis enheten din er koblet til My Kaspersky-kontoen din, vises e-postadressen din her.
3. Under abonnementsinformasjonen klikker du på de tre prikkene og velger **Skriv inn aktiveringskode**.
4. Skriv inn aktiveringskoden i feltet og klikk på **Lagre aktiveringskode**.

   Reserve-aktiveringskoden vises i vinduet **Abonnementsdetaljer**.

Hvis du skriver inn en reserve-aktiveringskode som ble utstedt for flere enheter, må du følge trinnene for å bruke reservekoden på alle enheter der du vil fornye abonnementet automatisk.

Det gjøres et forsøk på å aktivere og fullstendig bekrefte reservekoden når det gjeldende abonnementet utløper, eller hvis det gjeldende abonnementet fjernes fra enheten. Programmet bekrefter utløpsdatoen til reserve-aktiveringskoden, maksimalt antall enheter som abonnementet kan brukes på og kompatibiliteten til abonnementet med den installerte versjonen av programmet. Det kan være nødvendig å koble til My Kaspersky-kontoen din under aktivering av en reserve-aktiveringskode.

Hvis reserve-aktiveringskoden du legger til allerede er brukt på denne enheten, eller på en annen enhet, brukes datoen da programmet ble aktivert med denne koden for første gang som aktiveringsdato for fornyelse av abonnementet med reservekoden. Hvis du vil fornye abonnementet, legger du til en reserve-aktiveringskode som har en utløpsdato som er senere enn utløpsdatoen for abonnementet som brukes av programmet.

Hvis programmet ikke ble aktivert automatisk med en reserve-aktiveringskode, kan du aktivere det manuelt ved å klikke på **Prøv på nytt**-knappen. Hvis gjeldende abonnement er blokkert, kan du klikke på **Aktiver nå** for å aktivere programmet med en reserve-aktiveringskode.

Du kan også sende reserve-aktiveringskoden til enheter fra My Kaspersky-kontoen din. Se hjelpedelen for My Kaspersky for informasjon om hvordan du sender et abonnement til en enhet som er koblet til kontoen din.

Bytte fra prøveabonnement til betalt abonnement

Når den gratis prøveperioden utløper, fornyes og aktiveres abonnementet uten at du trenger å gjøre noe. Prisen for fornyelse av abonnement belastes betalingsmåten du har valgt.

I noen områder kan det hende at automatisk bytting til betalt abonnement ikke er tilgjengelig. Hvis du ikke oppga betalingsdetaljer for fornyelse da du abonnerte på den gratis prøveversjonen, må du kjøpe et abonnement for å sikre at enhetene dine forblir beskyttet.

Slik bytter du fra prøveabonnement til betalt abonnement:

1. Åpne hovedvinduet.
2. Gå til delen **Profil**. Hvis enheten din er koblet til My Kaspersky-kontoen din, vises e-postadressen din her.
3. Klikk på **Kjøp nå** i abonnementsinformasjonen.

   Nettstedet til Kaspersky eller en av våre partnere åpnes i standardnettleseren. Under kjøpsprosessen skriver du inn e-postadressen som er registrert for My Kaspersky-kontoen din.

Abonnementet du kjøpte, aktiveres automatisk på enheten din.

Slik installerer du programmet

Bruk veiviseren for installasjon og avinstallasjon til å installere programmet på maskinen i interaktiv modus.

Veiviseren består av en rekke vinduer (trinn). Antallet og rekkefølgen av trinn i veiviseren avhenger av området der du installerer programmet. I noen regioner ber veiviseren deg om å godta tilleggsavtaler om hvordan de personlige dataene dine behandles. Lukk veiviservinduet for å stanse veiviseren når som helst under installasjonen.

Hvis programmet skal beskytte mer enn én datamaskin (maksimalt antall datamaskiner er definert i sluttbrukerlisensavtalen), må det installeres likt på alle datamaskinene.

Slik installerer du programmet på datamaskinen:

- Hvis du bruker en installasjonsdisk, setter du inn disken i diskstasjonen og følger instruksjonene på skjermen.
- Hvis du har lastet ned programmet fra Internett, starter du det. Deretter installeres programmet ved hjelp av den standard installasjonsveiviseren. I dette tilfellet viser veiviseren flere andre installasjonstrinn for enkelte lokale språk.

Du kan også **installere programmet fra kommandolinjen**.

Du kan også installere Kaspersky-programmet fra kommandolinjen.

Enkelte kommandoer kan kun utføres under administratorkontoen.

Syntaks for kommandolinjen:

```
<bane til filen med installasjonspakken> [parametere]
```

Slik installerer du programmet fra kommandolinjen:

1. Åpne kommandolinjen som administrator.
2. Skriv inn banen til installasjonsfilen og kommandoen for å starte installasjonen med relevante alternativer og egenskaper. Installasjonsalternativer og egenskaper beskrives nedenfor.
3. Følg instruksjonene i installasjonsveiviseren.

Grunnleggende alternativer

Kommandonavn	Verdi	Eksempel
`/s`	Ikke-interaktiv (stille) modus: dialogbokser vises ikke under installasjonen.	`saas21.exe /s`
`/mybirthdate=YYYY-MM-DD`	Fødselsdato. Programmet installeres ikke hvis du er yngre enn 16. Dette alternativet er: • nødvendig for ikke-interaktiv installasjon • valgfritt for installasjon av programmet i OEM-modus	`saas21.exe /mybirthdate=1986-12-23`
`/l`	Velg språket som brukes for å installere den flerspråklige versjonen.	`saas21.exe /len-us`
`/t`	Mappe der installasjonsloggen er lagret.	`saas21.exe /tC:\KasperskyLab`
`/p<property>=<value>`	Angir installasjonsegenskaper.	`saas21.exe /pALLOWREBOOT=1 /pSKIPPRODUCTCHECK=1`
`/h`	Vis hjelp.	`saas21.exe /h`

Tilleggsinnstillinger

Kommandonavn	Verdi	Eksempel
/x	Fjern produktet.	`saas21.exe /x`

De viktigste installasjonsegenskapene

Kommandonavn	Verdi	Eksempel
`ACTIVATIONCODE=<value>`	Skriv inn aktiveringskoden.	
`AGREETOEULA=1`	Godta Lisensavtalen for sluttbrukere.	

AGREETOPRIVACYPOLICY=1	Godta personvernerklæringen.	
JOINKSN_ENHANCE_PROTECTION=1	Gi samtykke til sending av personopplysninger for å forbedre den grunnleggende funksjonaliteten til produktet.	
JOINKSN_MARKETING=1	Gi samtykke til sending av personopplysninger til markedsføringsformål.	
INSTALLDIR=<value>	Angi installasjonsplassering.	saas21.exe /p"INSTALLDIR=C:\Documents and Settings\saas21"
KLPASSWD=<value>	Angi passordet for ulike funksjoner i produktet. Hvis verdien KLPASSWDAREA ikke er angitt, brukes standard passordomfang: • Redigere programinnstillinger • Avslutte programmet	saas21.exe /pKLPASSWD=12345678
KLPASSWDAREA= [SET|EXIT|UNINST]	Angi passordomfanget som er konfigurert i KLPASSWD: • SET – Redigere programinnstillinger. • EXIT – Avslutte programmet. • UNINST – Fjerne programmet. Denne egenskapen kan ha flere verdier. I så fall må verdiene skilles med semikolon (;)	
SELFPROTECTION=1	Aktivere Selvforsvar under installasjonen.	saas21.exe /pSELFPROTECTION=1
ALLOWREBOOT=1	Tillate omstart om nødvendig.	saas21.exe /pALLOWREBOOT=1
SKIPPRODUCTCHECK=1	Ikke se etter programvare som er inkompatibel med Kaspersky.	saas21.exe /pSKIPPRODUCTCHECK=1
-oembackupmode	Ikke kjøre programmet etter installasjonen hvis Windows er startet i overvåkingsmodus.	saas21.exe /s -oembackupmode

Hvis du angir SKIPPRODUCTCHECK=1, har du selv alt ansvar for mulige konsekvenser av inkompatibilitet mellom Kaspersky og annen programvare.

Bruk SKIPPRODUCTCHECK=1 for å ignorere kun programmer som fjernes manuelt.

Eksempel på sammensatt kommando som gjør det mulig å starte datamaskinen på nytt under installasjonen og hoppe over søket etter inkompatibel programvare:

```
saas21.exe /pALLOWREBOOT=1 /pSKIPPRODUCTCHECK=1
```

Installasjonsveiviseren går gjennom følgende trinn:

1. Starter installasjonen

   I dette trinnet blir du automatisk spurt om du vil installere programmet.

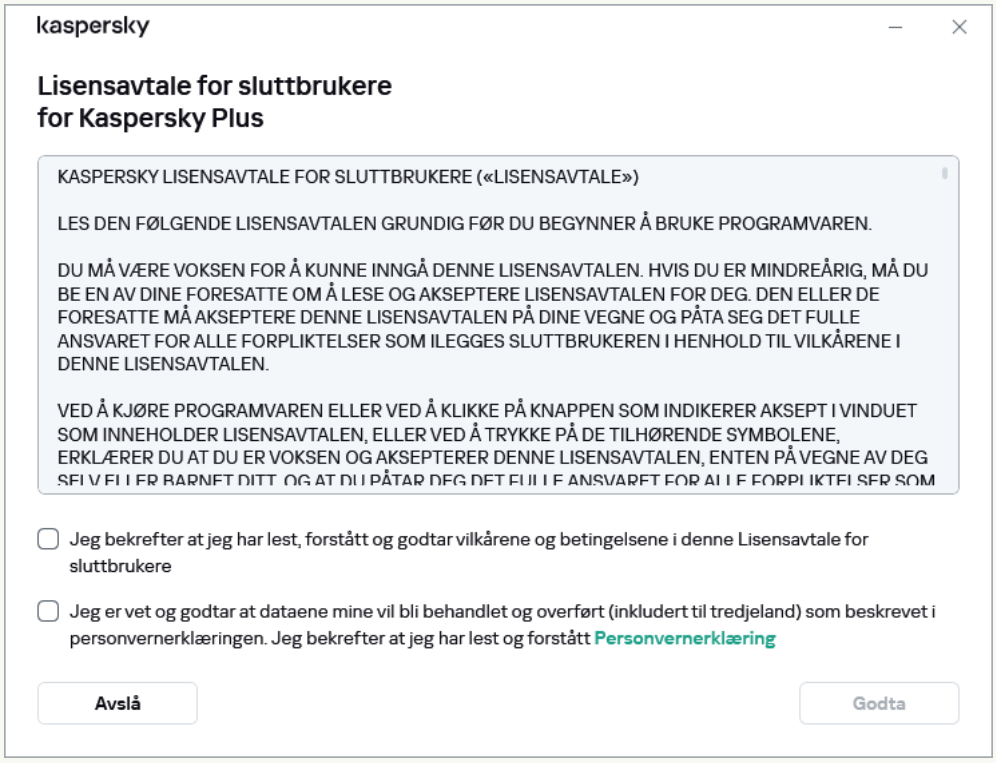
   Avhengig av installasjonstype og språk blir du spurt om du vil se lisensavtalen for sluttbrukere, som er inngått mellom deg og Kaspersky, i dette trinnet. Du blir også spurt om du vil delta i Kaspersky Security Network.

   Leser Lisensavtalen for sluttbrukere

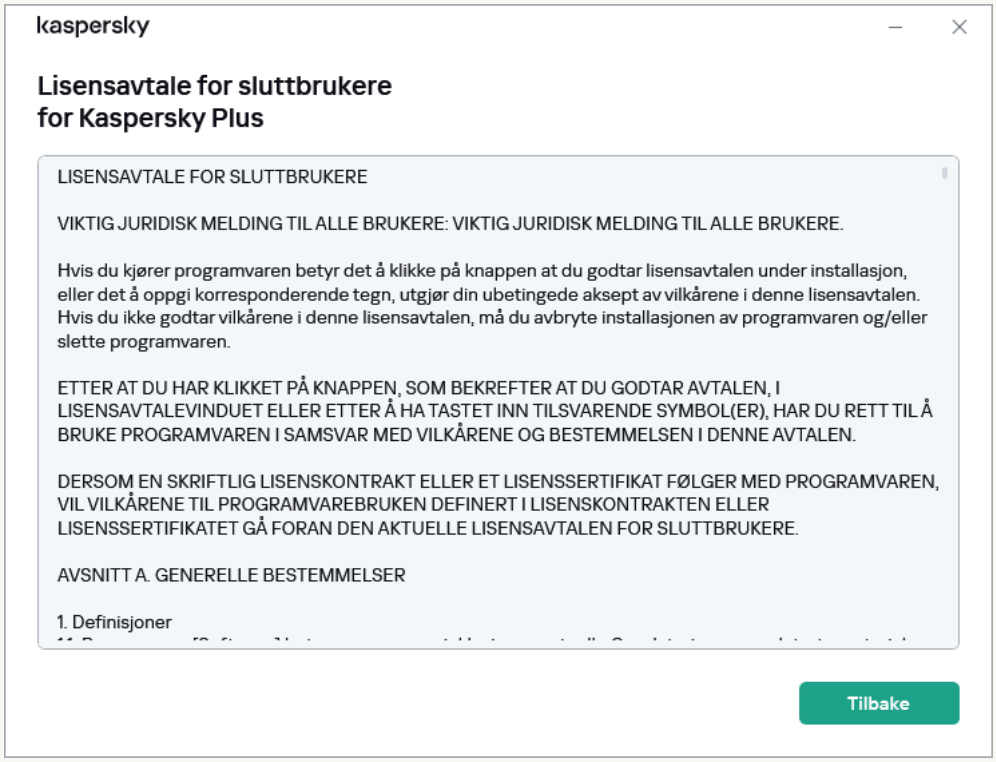
Dette trinnet i veiviseren vises for enkelte språk når du installerer programmet som er lastet ned fra Internett.

I dette trinnet blir du bedt om å se gjennom lisensavtalen for sluttbrukere, som er inngått mellom deg og Kaspersky.

Les lisensavtalen for sluttbrukere nøye. Hvis du godtar alle vilkårene i avtalen, klikker du på **Fortsett** (Denne knappen kalles **Godta** i enkelte områder).



I noen versjoner av programmet kan lisensavtale for sluttbrukere åpnes ved å klikke på koblingen på veiviserens velkomstskjerm. I dette tilfellet er det bare **Tilbake** knappen er tilgjengelig i vinduet som inneholder teksten til lisensavtalen for sluttbrukere. Ved å klikke på **Installer**-knappen, aksepterer du vilkårene i lisensavtale for sluttbrukere.



Installasjonen av programmet på datamaskinen vil da fortsette.

Hvis du ikke godtar lisensavtalen for sluttbrukere, installeres ikke programmet.

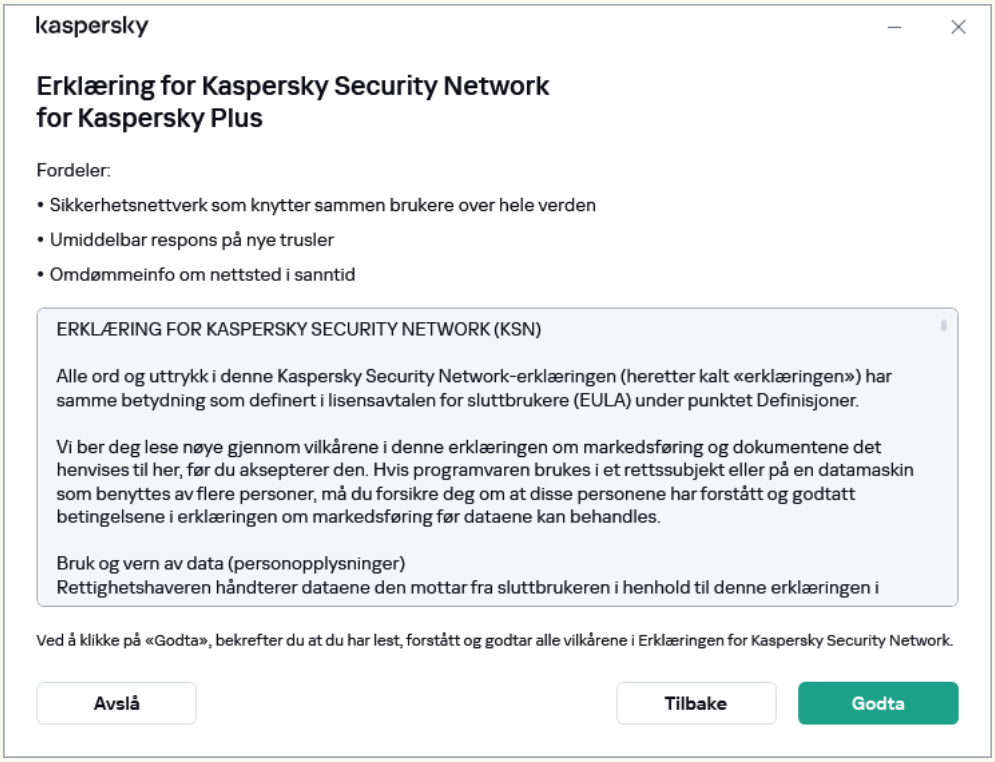
I noen regioner må du også godta vilkårene i personvernerklæringen for å fortsette installasjonen av programmet.

Ser gjennom personvernerklæringen for Kaspersky Security Network

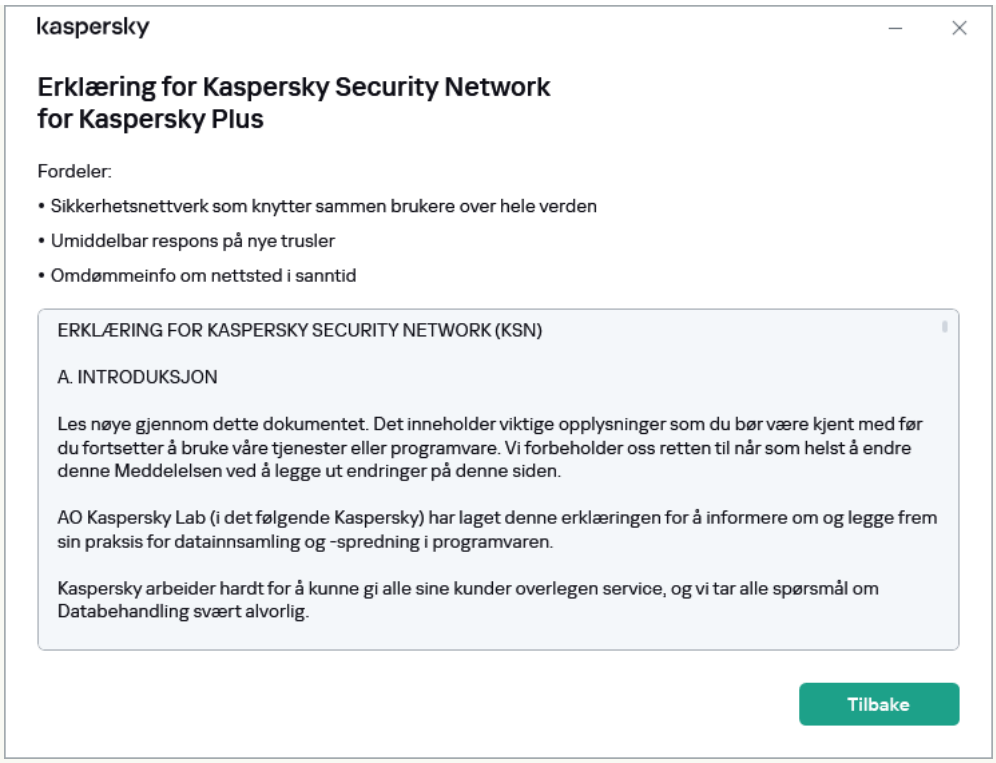
I dette trinnet inviteres du til å delta i Kaspersky Security Network. Deltakelse i programmet innebærer å sende informasjon om trusler oppdaget på datamaskinen, kjøre programmer og nedlastede signerte programmer og dele systeminformasjonen din med AO Kaspersky Lab. Ingen personlige data som mottas fra deg, blir samlet inn, behandlet eller lagret.

Les erklæringen for Kaspersky Security Network og gjør følgende:

- Hvis du godtar alle vilkårene, klikker du på **Godta**-knappen.
- Hvis du ikke ønsker å delta i Kaspersky Security Network, klikker du på **Avslå**.



I noen versjoner av programmet, må du aktivere avmerkingsboksen **Jeg vil delta i Kaspersky Security NetworkWELCOME_CHECK_PRIVACY_POLICY_PART1 = Vis** på velkomstskjermen til veiviseren, for å godta erklæringen for Kaspersky Security Network. Du kan lese erklæringen ved å klikke på lenken til **Kaspersky Security Network**. Etter at du har lest avtalen, klikker du på **Tilbake**-knappen for å fortsette installasjonen. Hvis avmerkingsboksen **Jeg vil delta i Kaspersky Security NetworkWELCOME_CHECK_PRIVACY_POLICY_PART1 = Vis** er valgt, godtar du vilkårene i erklæringen for Kaspersky Security Network ved å klikke på **Installer**-knappen.



Etter du har godtatt eller avslått deltakelse i Kaspersky Security Network, fortsetter installasjonen av programmet.

I programversjoner inkluderer Kaspersky Security Network-erklæringen informasjon om behandling av personlige data.

2. Installere programmet

   Installasjon av programmet kan ta litt tid. Vent til det er fullført. Når installasjonen er fullført, fortsetter installasjonsveiviseren automatisk til neste trinn.

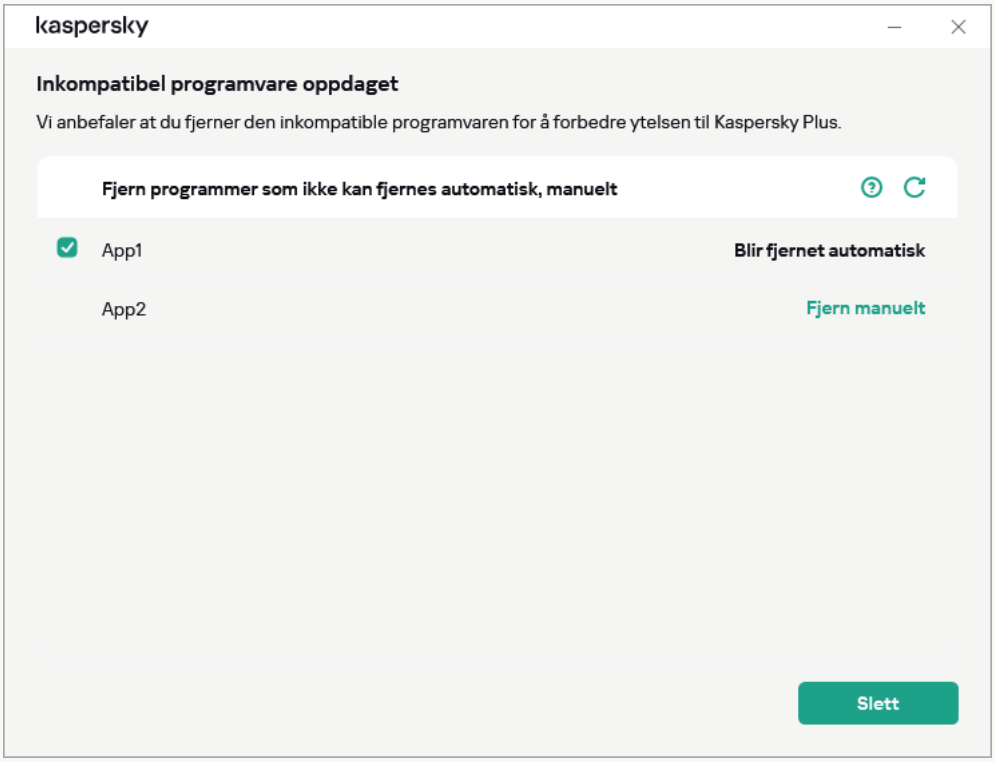
   Kontroller under installasjon av programmet

Programmet foretar flere kontroller under installasjonen. Disse kontrollene kan finne følgende problemer:

- *Operativsystemet fungerer ikke i henhold til programvarekravene*. Under installasjonen kontrollerer veiviseren følgende:
  - Om operativsystemet og oppdateringspakkene fyller programvarekravene
  - Alle nødvendige programmer er tilgjengelige
  - Den ledige diskplassen er tilstrekkelig for installasjonen
  - Brukeren som installerer programmet, har administratorrettigheter

  Hvis noen av kravene ovenfor ikke oppfylles, vises en korresponderende varsling.

- *Det finnes inkompatible programmer på datamaskinen*. Hvis noen inkompatible programmer oppdages, vises de i en listen på skjermen, og du blir bedt om å fjerne dem. Programmer som ikke kan fjernes automatisk, må fjernes manuelt ved å klikke på **Fjern manuelt**-knappen.



Ved fjerning av inkompatible programmer, må du starte operativsystemet på nytt, hvoretter installasjon av Kaspersky vil fortsette automatisk.

Installere Kaspersky Password Manager sammen med Kaspersky Plus eller Kaspersky Premium

Før installasjonen fullføres, vil Kaspersky også be deg om å installere Kaspersky Password Manager for å beskytte passordene dine. Installasjonen av Kaspersky Password Manager kan fortsette etter at Kaspersky er ferdig installert – du får ikke en egen varsling om at installasjonen av Kaspersky Password Manager er fullført.

Kaspersky Password Manager er ikke inkludert i Kaspersky Basic og Kaspersky Standard. Hvis du vil bruke Kaspersky Password Manager til passordbeskyttelse, kan du laste ned og installere det som et eget program eller bytte til Kaspersky Plus.

3. Fullfører installasjonen

   Dette trinnet i veiviseren informerer deg om fullførelsen av programinstallasjonen.

   Alle nødvendige programkomponenter startes automatisk etter at installasjonen er fullført.

   I noen tilfeller må du starte datamaskinen på nytt for å fullføre installasjonen.

Både programmet og plugin-moduler for nettlesere installeres for å gi sikker surfing på nett.

Når du kjører opptaks- eller avspillingsprogrammer for lyd- og video for første gang etter at du har installert Kaspersky, er det mulig at disse opptakene eller avspillingene avbrytes. Det er nødvendig for å aktivere funksjonen som kontrollerer programmenes tilgang til lydopptaksenheter. Systemtjenesten som kontrollerer lydmaskinvare startes på nytt når Kaspersky kjører for første gang.

Kaspersky Plus eller Kaspersky Premium installeres sammen med Kaspersky VPN Secure Connection, et program beregnet på å etablere en sikker tilkobling via Virtual Private Network (VPN). Du kan fjerne Kaspersky VPN Secure Connection uavhengig av Kaspersky-programmet. Hvis bruk av VPN er forbudt i landet du bor i, vil Kaspersky VPN Secure Connection ikke bli installert.

Hvis du lastet ned programmet fra My Kaspersky-kontoen din, aktiveres programmet automatisk med abonnementet fra kontoen din etter at installasjonen er ferdig.

Installere over andre Kaspersky-programmer

Programmet kan installeres over følgende Kaspersky-programmer:

- Kaspersky Free
- Kaspersky Anti-Virus
- Kaspersky Internet Security
- Kaspersky Total Security
- Kaspersky Security Cloud

Når du installerer det nye programmet, fjernes tidligere installerte Kaspersky Anti-Virus-, Kaspersky Internet Security-, Kaspersky Security Cloud-, Kaspersky Total Security-programmer. Lisensen til et fjernet program kan brukes for det nye Kaspersky-programmet, med unntak av Kaspersky Total Security-lisensen. Innstillingene for fjernede programmer beholdes.

Når du installerer det nye programmet, fjernes det tidligere installerte Kaspersky Free-programmet. Innstillingene for Kaspersky Free lagres ikke.

Når du bytter fra Kaspersky Total Security til Kaspersky Basic eller Kaspersky Standard, beholdes det sikkerhetskopier av filene, men de vises ikke i disse programmene. Du kan legge til sikkerhetskopier av filer manuelt. Når du bytter fra Kaspersky Total Security til Kaspersky Plus, beholdes kopier av filer og vises automatisk.

Nettleserutvidelse for Kaspersky Protection

Du må installere og aktivere Kaspersky Protection-utvidelsen i alle nettlesere du bruker, for at Kaspersky skal kunne støtte disse nettleserne fullstendig. Utvidelsen for Kaspersky Protection setter inn skript i nettsider som åpnes i Beskyttet nettleser og i trafikken. Programmet bruker dette skriptet til å samhandle med nettstedet og overføre data til banker med nettsteder som beskyttes av komponenten Safe Money. Programmet bruker en digital signatur til å beskytte dataene som overføres av skriptet. Programmet kan legge inn skriptet uten å bruke Kaspersky Protection-utvidelsen.

Programmet signerer dataene som overføres av skriptet med de installerte antivirus-databasene og forespørsler til Kaspersky Security Network. Programmet sender forespørsler til Kaspersky Security Network, uavhengig av hvorvidt du har godtatt vilkårene i personvernerklæringen for Kaspersky Security Network.

Kaspersky Protection-utvidelsen gjør følgende når du jobber i nettleseren:

Administrerer Privat surfing.

Administrerer Anti-Banner.

Informerer om mistenkt phishing.

Slik rapporterer du et nettsted du mistenker for phishing:

1. Sørg for at du er på siden du mistenker er en phishing-side.
2. I verktøylinjen i nettleseren klikker du på **Kaspersky Protection**.
3. I menyen for utvidelsen velger du **Informer om mistenkt phishing**.
4. Dette åpner et vindu. Sørg for at vinduet viser nettadressen til nettstedet du mistenker for phishing.
5. Klikk på **Informer**.

   Rapporten sendes til Kaspersky Security Network.

Informer om problem på nettsted

Slik informerer du om et problem på nettsteder:

1. Sørg for at du er på siden du vil rapportere som problematisk.
2. I verktøylinjen i nettleseren klikker du på **Kaspersky Protection**.
3. I menyen for utvidelsen velger du **Fortell om problemer med nettsiden**.
4. Dette åpner et vindu. Sørg for at vinduet viser nettadressen til nettstedet.
5. Beskriv problemet i tekstboksen.
6. Klikk på **Informer**.

   Meldingen er levert.

Åpne Skjermtastatur

Installere utvidelsen for Kaspersky Protection i Chromium-basert Microsoft Edge, Mozilla Firefox og Google Chrome

I nettleserne Google Chrome og Mozilla Firefox installeres utvidelsen for Kaspersky Protection automatisk. Kaspersky ber deg om å aktivere utvidelsen. I den Chromium-baserte Microsoft Edge-nettleseren installeres også utvidelsen for Kaspersky Protection automatisk, men programmet ber deg ikke om å aktivere utvidelsen. Du må aktivere utvidelsen selv.

Støtte for Yandex Browser

Når du bruker Yandex Browser, kjører følgende programkomponenter:

- Beskyttet Nettleser
- URL-veileder
- Sikker surfing
- Anti-Phishing

Komponentene Privat surfing og Anti-Banner kjører, men kan ikke konfigureres i Yandex Browser.

Støtte for Internet Explorer

Fra og med versjon 4 av Kaspersky-programmet støtter ikke Kaspersky Protection-utvidelsen nettleseren Internet Explorer lenger. Hvis du vil fortsette å bruke Kaspersky Protection-funksjonen i Internet Explorer, kan du gå tilbake til forrige versjon av programmet.

Slik avinstallerer du programmet

Etter at du har avinstallert programmet, vil datamaskinen og personopplysningene dine ikke lenger være beskyttet.

Du kan fjerne programmet ved å bruke installasjonsveiviseren.

Slik avinstallerer du programmet i Windows 7

Du kan starte veiviseren på datamaskiner med Microsoft Windows 7 eller eldre versjoner ved å

gå til **Start**-menyen og velge **Alle programmer** → **Kaspersky** → **Fjern Kaspersky**.

Slik avinstallerer du programmet i Windows 8 eller senere

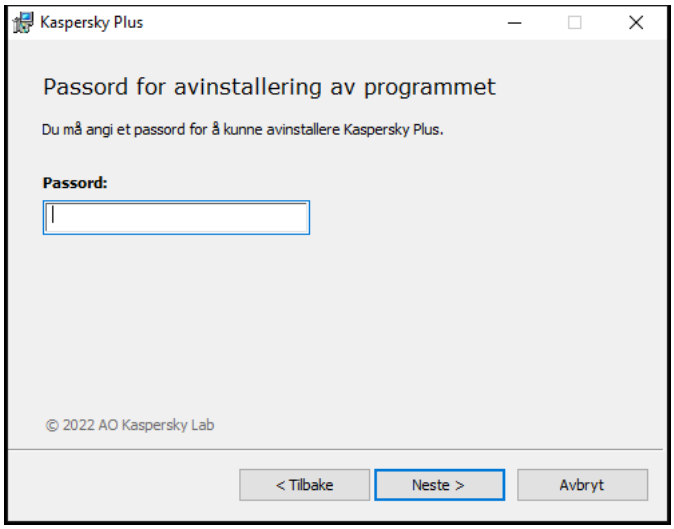
Slik starter du veiviseren på en datamaskin med Microsoft Windows 8 eller nyere:

1. Finn det installerte programmet på en av følgende måter:
   - I Windows 8 klikker du på **Start**-knappen og velger Kaspersky-programmet på hurtigstart-skjermen.
   - I Windows 10 og nyere klikker du på **Start** for å finne programmet i listen eller ved å bruke søkefeltet.
2. Høyreklikk på snarveien til Kaspersky-programmet.
3. I kontekstmenyen velger du **Avinstaller**.
4. Velg Kaspersky i listen i vinduet som åpnes.
5. Klikk på **Fjern** / **Rediger** nederst i vinduet.

Installasjonsveiviserent vil starte.

Fjerning innebærer følgende trinn:

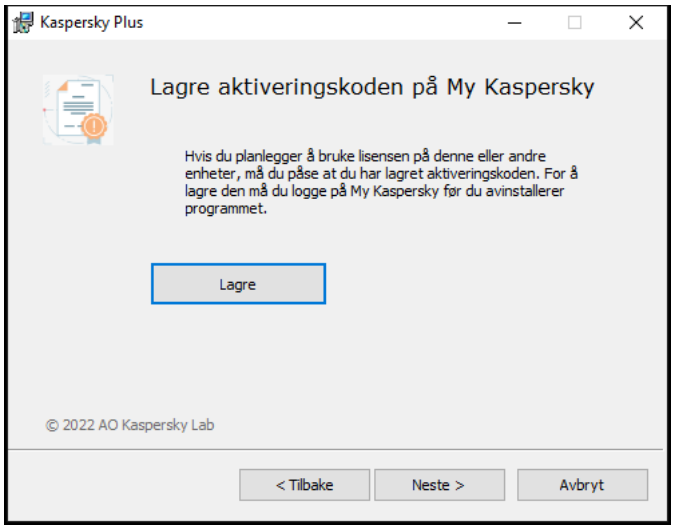
1. Hvis du vil fjerne programmet, må du angi passordet som gir deg tilgang til programinnstillingene. Hvis du av en eller annen årsak ikke kan angi passordet, vil fjerning av programmet være forbudt. Etter at du har skrevet inn passordet, klikker du på **Bekreft**.



Dette trinnet er bare tilgjengelig hvis det er angitt et passord for fjerning av programmet.

2. Lagre et abonnementet på My Kaspersky-kontoen din.

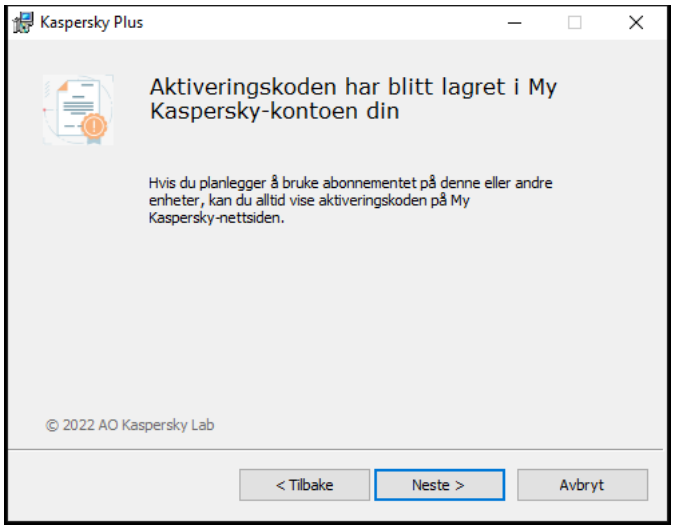
   I dette trinnet kan du spesifisere om du vil lagre abonnementet på My Kaspersky-kontoen din for fremtidig bruk.



   a. Hvis du vil lagre et abonnement, klikker du på **Lagre**.

   b. Klikk på **Neste >**.

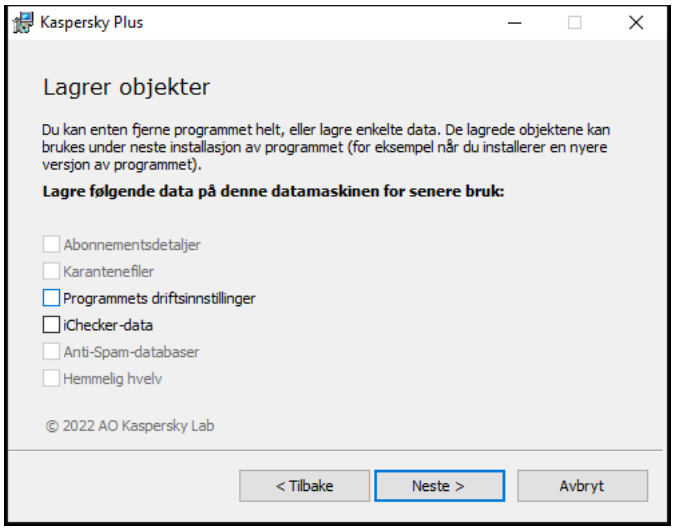
   Vinduet med det lagrede abonnementet vises.



   a. Klikk på **Neste >**.

3. Lagre data for fremtidig bruk

   På dette tidspunktet kan du angi hvilke data som benyttes av programmet, som du vil beholde for gjentatt bruk under neste installasjon av programmet (f.eks. når du installerer en nyere programversjon).



Du kan lagre følgende data:

- **Abonnementsdetaljer** er et sett med data som fjerner behovet for å aktivere det nye programmet. Du kan bruke programmet med det gjeldende abonnementet, med mindre abonnementet utløper før du starter installasjonen.
- **Karantenefiler** – filer som er skannet av programmet og flyttet til Karantene.

  Hvis programmet fjernes fra datamaskinen, blir filer i Karantene utilgjengelige. Kaspersky-programmet må være installert for å utføre handlinger med disse filene.

- **Programmets driftsinnstillinger** er verdier for programinnstillinger som velges når programmet konfigureres.

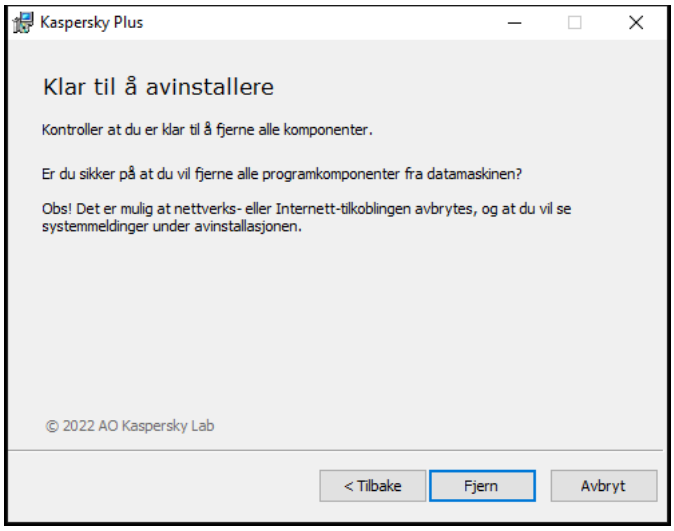
Du kan også eksportere beskyttelsesinnstillingene på kommandolinjen ved hjelp av følgende kommando: `avp.com EXPORT <filnavn>`.

- **iChecker-data** – filer som inneholder informasjon om objekter som allerede er skannet med iChecker-teknologi.
- **Anti-Spam-databaser** – databaser med eksemplarer av spam-meldinger lagt til av brukeren.
- **Hemmelig hvelv** er filer som er lagret ved hjelp av funksjonen Hemmelig hvelv.

Klikk på **Neste >** for å fortsette å avinstallere programmet.

4. Bekrefte fjerning

   Fjerning av programmet vil påvirke sikkerheten til datamaskinen og personlige data, du vil derfor bli bedt om å bekrefte at du ønsker å slette programmet. Det gjør du ved å klikke **Fjern**-knappen.



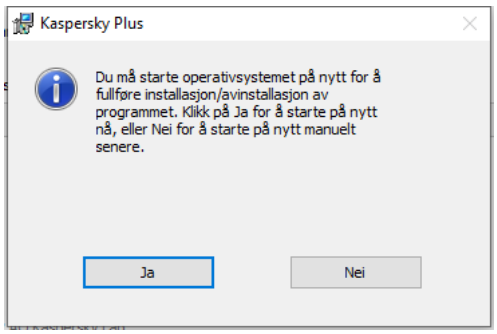
5. Fullføre fjerningen

   På dette trinnet fjerner veiviseren programmet fra datamaskinen. Vent til fjerningen er fullført.

   > Denne funksjonaliteten kan være utilgjengelig i enkelte regioner.

   Du må starte operativsystemet på nytt under fjerning av programmet. Hvis du avbryter den umiddelbare omstarten, blir ikke avinstallasjonen fullført før neste gang du starter operativsystemet eller når du slår av og på datamaskinen igjen.

6. Klikk på **Ja** for å starte datamaskinen på nytt.



Slik oppdaterer du programmet

Programmet oppdateres automatisk hvis du velger oppdateringsmodusen **Automatisk** i vinduet for oppdateringsinnstillinger (**Sikkerhet** → **Oppdatering av antivirusdatabaser** → **Tidsplan for oppdatering av databaser**).

Programmet oppdateres automatisk hvis du installerer en ny versjon av programmet over den forrige.

Slik beskytter du flere enheter

Kun tilgjengelig i Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Du kan bruke abonnementet til å beskytte alle enheter som kjører operativsystemene Microsoft Windows, Android, iOS og macOS. Det nøyaktige antallet enheter du kan bruke abonnementet var spesifisert i egenskapene for abonnementet da du kjøpte det.

Du kan alltid sjekke hvor mange enheter du allerede beskytter, og hvor mange flere du kan beskytte i **Profil**-delen av programmet, samt i My Kaspersky-kontoen din. Der finner du også brukervennlige verktøy for å dele beskyttelsen din med andre enheter.

Du trenger ikke å huske aktiveringskoden for dele beskyttelsen fra disse verktøyene, da abonnementet overføres via kontoen din. Hvis du aldri har logget på My Kaspersky-kontoen din på den aktuelle enheten, vil vi be deg om å gjøre det som en del av prosessen. Etter installasjon aktiveres programmene dine automatisk med abonnementet fra kontoen din.

Slik deler du beskyttelse fra programmet ditt:

1. Åpne hovedvinduet.
2. Gå til delen **Profil**.
3. Klikk på denne knappen +. I noen abonnementer, er teksten **Beskytt enhet** skrevet på knappen.
4. Velg ett av følgende alternativer i **Beskytt flere enheter**-vinduet:

   - **Skann en QR-kode**

     Rett telefonens kamera mot QR-koden i **QR-kode**-fanen.

     Dette vil åpne Google Play-butikken, App Store eller Huawei AppGallery via appnedlastingssiden på den mobile enheten din. Etter at du har lastet ned og installert programmet, kobles det automatisk til My Kaspersky og begynner å beskytte enheten din.

     > Ved å bruke en QR-kode på en Android-enhet godtar du å oppgi et engangspassord til Google Play for å aktivere programmet på smarttelefonen din.

   - **Send en lenke på e-post**

     a. Gå til **På e-post**-fanen.

     b. Klikk på koblingen.

     Dette åpner My Kaspersky-påloggingsvinduet i standardnettleseren din.

     c. I **Send via e-post** -vinduet skriver du inn e-postadressen i tekstboksen og klikker **Send**.

     d. Last ned programmet ved å følge lenken i e-posten.

     Etter nedlasting og installasjon, kobles programmet automatisk til My Kaspersky-kontoen din.

> I noen abonnementsplaner kan bare den generelle informasjonen om det totale antallet enheter du kan beskytte vises.

Se hjelpedelen for My Kaspersky for mer informasjon om ekstern administrasjon av enhetenes beskyttelse, tilbakekalling av abonnement fra en bruker eller tilbakekalling av abonnementet fra en enhet.

Grunnleggende funksjoner i programmet

I denne delen vil du lære om grunnleggende konfigurering av programmet, inkludert konfigurering av varsler og brukergrensesnitt og hvordan du løser sikkerhetsproblemer som kan oppstå.

Vurdere datamaskinens beskyttelsesstatus og løse sikkerhetsproblemer

Problemer med beskyttelse av datamaskinen angis ved hjelp av en indikator øverst i hovedvinduet. Grønt indikerer at datamaskinen er beskyttet. Gult indikerer at det er problemer med beskyttelsen, og rødt indikerer at datamaskinens sikkerhet er i alvorlig fare. Vi anbefaler at du fikser problemene og truslene umiddelbart.

Du kan åpne vinduet **Varslingssenter** ved å klikke på knappen **Detaljer** i hovedvinduet. Dette vinduet gir detaljert informasjon om datamaskinens beskyttelsesstatus og foreslår mulige tiltak for å rette opp problemer og trusler.

Problemer knyttet til beskyttelsen grupperes etter kategorier. En liste med handlinger vises for hvert problem, som du kan utføre for å løse problemet.

Delen **Status** viser informasjon om datamaskinens beskyttelses og abonnementsstatus. Hvis det oppdages problemer som må rettes opp, vises **Reparer** vises ved siden av varslingen. Du kan rette opp sikkerhetsproblemer ved å klikke på denne knappen.

Delen **Anbefalinger** viser en liste over handlinger som skal utføres for å optimalisere programytelsen og bruke den mer effektivt.

Delen **Nyheter** viser nyheter om cybersikkerhet.

Hvis du klikker på **Vis N ignorerte varsler**, vises varslinger som handlingen **Ignorer** har blitt brukt for. Ignorerte varslinger påvirker ikke fargen på beskyttelsesindikatoren i hovedvinduet.

Slik reparerer du sikkerhetsproblemer på PC-en

Slik reparerer du sikkerhetsproblemer på PC-en:

1. Åpne hovedvinduet.
2. Klikk på **Detaljer** øverst i hovedprogramvinduet for å gå til vinduet **Varslingssenter**.
3. Gå til delen **Status**. Denne delen viser sikkerhetsproblemer på PC-en.
   - Velg et problem fra listen og klikk på en handlingsknapp, f.eks **Reparer**.
   - Velg **Ignorer** fra rullegardinlisten hvis du ikke vil løse dette problemet nå. Du kan se listen over ignorerte varsler senere ved å klikke på knappen **Vis N ignorerte varslinger**.
4. Gå til delen **Anbefalinger**. Denne delen viser anbefalinger som ikke er obligatoriske, men som vil hjelpe deg med å optimalisere bruken av programmet og gi bedre beskyttelse for PC-en.
   a. Velg et forslag fra listen.
   b. Klikk på knappen ved siden av en foreslått handling, for eksempel **Aktiver** ved siden av forslaget **Vil du bli kvitt irriterende reklame?**.

5. Gå til delen **Nyheter**. I denne delen finner du nyheter om cybersikkerhet. Bruk navigasjonsknappene for å gå til neste nyhet eller gå tilbake til forrige nyhet.

Sikkerhetsnyheter

Denne delen inneholder informasjon om sikkerhetsnyheter fra Kaspersky.

Om sikkerhetsnyheter

Hver dag skjer det flere og flere massetyverier av passord, hacking av databaser og nettbanksvindler rundt om i verden. Kasperskys sikkerhetsnyheter gir oppdatert informasjon om slike forbrytelser, og hjelper deg med å unngå situasjoner der du kan bli offer for hackere. For å sikre at du mottar sikkerhetsnyheter som er relevante, vil programmet analysere informasjon om ressursene du besøker og programmene du bruker. Denne informasjonen brukes kun til å plukke ut nyheter som kan være viktige eller interessante for deg.

Sikkerhetsnyheter vises i varslingssenteret, sammen med andre nyheter fra Kaspersky. Sikkerhetsrelaterte nyhetsvarsler vises i systemstatusfeltet. Varslingsvinduer inneholder nyhetsoverskrifter og en kort anbefaling for hvordan problemet som beskrives i nyhetene kan løses.

Du kan bli vist følgende typer nyheter, avhengig av sikkerhetsnivået:

- *Viktige nyheter* – nyheter om hendelser som utgjør en potensiell sikkerhetstrussel (for eksempel nyheter om massetyveri av Facebook-passord). Vinduer med viktige nyheter er gule.
- *Generelle nyheter* – nyheter med informasjon (for eksempel nyheter om stadig hyppigere tilfeller av brudd på datasikkerheten i nettbanker, forårsaket av skadelige trojanere). Vinduer med generelle nyheter er grønne.

Hvis et varsel om sikkerhetsnyheter vises på skjermen, kan du vise hele teksten i artikkelen ved å klikke på **Detaljer** i popup-vinduet, eller lukke vinduet hvis du ikke ønsker mer informasjon. Du kan når som helst vise hele teksten i nyhetsartikler ved å velge de aktuelle nyhetene i nyhetslisten i varslingssenteret.

Hvis du ikke ønsker å motta sikkerhetsnyheter på en bestemt enhet, kan du deaktivere visning av nyheter. Hvis du ikke ønsker å motta nyheter på noen av enhetene dine, deaktiverer du mottak av nyheter på My Kaspersky.

Sikkerhetsnyheter vises den første timen programmet brukes etter installasjon.

Slik aktiverer eller deaktiverer du sikkerhetsnyheter

Slik aktiverer eller deaktiverer du sikkerhetsnyheter:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Innstillinger for grensesnitt**.

Vinduet **Innstillinger for grensesnitt** vil da åpne.

4. Gjør ett av følgende i vinduet **Reklamemateriell**:

   - Hvis du vil motta sikkerhetsnyheter, aktiverer du alternativet **Motta informasjonsmeldinger og reklamer fra Kaspersky**.
   - Hvis du ikke vil motta sikkerhetsnyheter, deaktiverer du alternativet **Motta informasjonsmeldinger og reklamer fra Kaspersky**.

Slik aktiverer og deaktiverer du mottak av sikkerhetsnyheter i My Kaspersky

Slik aktiverer og deaktiverer du mottak av sikkerhetsnyheter på My Kaspersky:

1. Åpne hovedsiden i My Kaspersky.
2. Klikk på **Logg på** og angi e-postadressen og passordet du oppga da du opprettet kontoen din.
3. Klikk på denne knappen .
   Dette åpner vinduet for visning av varsler.
4. Klikk på **Innstillinger** for å gå til vinduet Varslingsinnstillinger.
5. Gjør ett av følgende:

   - Hvis du vil aktivere mottak av sikkerhetsnyheter, aktiverer du alternativet **Sikkerhetsnyheter**.
   - Hvis du vil deaktivere mottak av sikkerhetsnyheter, deaktiverer du alternativet **Sikkerhetsnyheter**.

Programaktivitetslogg og detaljert rapport

I hovedvinduet kan du se en kort oversikt over alle handlinger som utføres av programmet mens det brukes. Denne informasjonen hjelper deg med å forstå nøyaktig hvordan programmet beskytter enheten din og dataene dine.

Slik viser du tidslinjen:

1. Åpne hovedvinduet.
   I delen **Hjem**, like under **Tidslinje**, ser du en kort aktivitetshistorikk for programmet.
2. Klikk på **Vis alle** for å se aktivitetshistorikken for programmet.
   Dette åpner et vindu med en detaljert beskrivelse av handlinger utført av programmet, og tidspunktet da hendelser inntraff.
3. Klikk på **Vis rapporter** for å se en detaljert rapport om programmet.
   Dette tar deg til vinduet **Rapporter**.

Du kan også se den detaljerte rapporten ved å klikke på **Rapporter** i delen **Sikkerhet**. Vinduet **Rapporter** viser data i form av en tabell. Du kan tilpasse visningen av rapporter ved å velge ulike filtreringsalternativer.

Slik konfigurerer du programgrensesnittet

Denne delen inneholder informasjon om hvordan du konfigurerer grensesnittet til programmet.

Slik konfigurerer du programvarslinger

Meldinger som vises i systemstatusfeltet, informerer deg om programhendelser som krever din oppmerksomhet. Du kan motta følgende varslinger avhengig av hvor kritisk hendelsen er:

- *Kritiske varslinger* – informerer deg om hendelser av avgjørende viktighet for datamaskinens sikkerhet, for eksempel oppdagelse av et skadelig objekt eller farlig aktivitet i operativsystemet. Vinduer med kritiske varslinger og popup-meldinger vises i rødt.

- *Viktige varslinger* – informerer deg om hendelser som er potensielt viktige med hensyn til datamaskinens sikkerhet, for eksempel oppdagelse av et potensielt infisert objekt eller mistenkelig aktivitet i operativsystemet. Vinduer med viktige varslinger og popup-meldinger vises i gult.

- *Informasjonsvarslinger* – informerer deg om hendelser som ikke er kritisk viktige for datamaskinens sikkerhet. Meldingsvinduet og popup-meldinger vises i grønt.

Hvis du ser en varsling på skjermen, bør du velge en av de anbefalte handlingene i varslingen. Det beste valget det som er anbefales som standard av Kasperskys eksperter.

En varsling kan lukkes automatisk når datamaskinen startes på nytt, når Kaspersky-programmet avsluttes eller i tilkoblet ventemodus i Windows 8. Varslinger fra Inntrengningsbeskyttelse lukkes automatisk etter 500 sekunder. Varsling om oppstart av programmet lukkes etter 1 time. Når en varsling lukkes automatisk, utfører Kaspersky-programmet handlingen som er anbefalt som standard.

Klikk på lenkene nedenfor for å lese hvordan du konfigurerer programvarslinger.

Slik konfigurerer du levering av varslinger

Slik oppretter du varslingsregler:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Innstillinger for grensesnitt**.
4. I blokken **Varslinger** klikker du på **Varslingsinnstillinger** for å fortsette til vinduet for varslingsinnstillinger.
5. Velg komponenten i listen til venstre.
   Delen til høyre i vinduet viser en liste over hendelser som kan oppstå under bruk av denne komponenten.
6. Velg en hendelse fra listen og velg følgende alternativer:

   - **Lagre i lokal rapport**. Når hendelsen inntreffer, skrives informasjon om den til en rapport som lagres på den lokale datamaskinen.
   - **Varsle på skjermen**. Når hendelsen inntreffer, vises et popup-varsel over programikonet i systemstatusfeltet.

   Du kan bruke rullegardinlisten nederst til venstre for å angi hvilke varsler du vil lagre i den lokale rapporten:

   - **Standard**. Når dette alternativet er valgt, lagrer den genererte rapporten hendelser valgt av Kasperskys eksperter.
   - **Manuelt**. Dette alternativet velges automatisk hvis du konfigurerer muligheten til å lagre hendelser manuelt i en rapport.
   - **Kritisk**. Når dette alternativet er valgt, lagrer den genererte rapporten **Kristiske hendelser** (inkludert *Applikasjonsfeil hendelser* for komponentene **Systemrevisjon** og **Inntrengningsbeskyttelse**).
   - **Viktig**. Når dette alternativet er valgt, lagrer den genererte rapporten **Kristiske hendelser** (inkludert *programfeil-hendelser* for komponentene **Systemrevisjon** og **Inntrengningsbeskyttelse**) og **Advarsler**.
   - **Informativ**. Når dette alternativet er valgt, lagrer den genererte rapporten alle hendelser.

Varsler om alle endringer som er relatert til hendelsen **Programmet jobber og behandler data i henhold til relevante lover og bruker den nødvendige infrastrukturen**, vises alltid på skjermen i oppgavelinjeområdet. Innstillingen endres ikke hvis du deaktiverer avmerkingsboksen.

Slik konfigurerer du levering av varslinger med nyheter og spesialtilbud fra Kaspersky

Slik holder du deg informert om det siste innen cybersikkerhet og motta spesialtilbud fra Kaspersky:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Gå til delen **Innstillinger for grensesnitt**.
4. Velg alternativet **Nyhetsvarsler** hvis du vil **Motta informasjonsmeldinger og reklamer fra Kaspersky** hvis du vil motta varsler om nyheter innen datamaskinsikkerhet.
5. Gjør ett av følgende i vinduet **Reklamemateriell**:
   - Velg **Motta informasjonsmeldinger og reklamer fra Kaspersky** avkrysningsboksen hvis du vil motta varsler om nyheter innen datamaskinsikkerhet.
   - Velg alternativet **Vis informasjon om spesialtilbud på nettstedet** hvis du ønsker å motta de beste tilbudene når du besøker Kasperskys nettsteder.
   - Velg alternativet **Motta informasjonsmeldinger og reklame etter at gjeldende abonnement utløper** hvis du ønsker å motta varsler om sikkerhetsnyheter fra Kaspersky etter at abonnementet ditt utløper.

Slik aktiverer du varslingslyder

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Innstillinger for grensesnitt**.
4. I blokken **Varslinger** velger du alternativet **Aktiver varsellyder**.
   Hvis du vil endre standardlydsignalet til «grisehyl», må du skrive **IDKFA** i **Om**-vinduet.

Det avgis ingen lydsignaler for varslinger i Microsoft Windows 10.

Slik konfigurerer du varslinger om at et barn bruker programmet

Hvis Kaspersky Safe Kids er installert på datamaskinen, kan du aktivere eller deaktivere Kaspersky-varslinger om at et barn bruker datamaskinen.

Slik konfigurerer du varslinger om at et barn bruker programmet:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Gå til delen **Innstillinger for grensesnitt**.
4. Velg et alternativ:
   - Deaktiver alternativet **Vis varslinger i barnas kontoer** for å slå av Kaspersky-varslinger når et barn bruker programmet.
   - Velg alternativet **Vis varslinger i barnas kontoer** for å slå på Kaspersky-varslinger når et barn bruker programmet.

Detaljer om hvordan du konfigurerer Kaspersky-programmet når et barn bruker en datamaskin.

Slik endrer du programmets designtema

Muligheten til å endre temaet for programmets designtema er ikke tilgjengelig i noen regioner.

Slik endrer du programmets designtema:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Innstillinger for grensesnitt**.
4. I blokken **Designtema**, velger du ett av følgende alternativer:
   - **Samme som operativsystemet**. Det gjeldende designtemaet for operativsystemet brukes.
   - **Lyst**. Det lyse designtemaet for programmet brukes.
   - **Mørkt**. Det mørke designtemaet for programmet brukes.
   - **Bruk et tema med egendefinert design**, hvis du vil bruke et tilpasset designtema. Klikk på **Velg** og skriv inn banen til ZIP-arkivet eller mappen der filene med det egendefinerte designtemaet ligger.

Designtemaet iverksettes etter omstart av programmet.

Slik konfigurerer du programikonet

I denne delen lærer du hvordan du konfigurerer programikonet på skrivebordet og i systemstatusfeltet.

Slik endrer du programikonet

Slik endrer du programikonet:

1. Åpne hovedvinduet.
2. Klikk på ⚙ -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Innstillinger for grensesnitt**.
4. I blokken **Programikon**, velger du ett av følgende alternativer:

   - **Standardikon**. Når dette alternativet er valgt, viser skrivebordet og varslingsområdet det standard programikonet.
   - **Midori Kuma**. Når dette alternativet er valgt, viser skrivebordet og varslingsområdet ikonet med et bilde av Midori Kuma, bjørnemaskotten vår.

Hvis du vil gå tilbake til det tradisjonelle programikonet med bokstaven K, skriver du **IDDQD** i vinduet **Om**. Du må starte datamaskinen på nytt for å ta i bruk endringene.

Slik endrer du ikonet i systemstatusfeltet, avhengig av beskyttelsesstatus

Slik endrer du Kaspersky-programikonet i systemstatusfeltet, avhengig av programstatus:

1. Åpne hovedvinduet.
2. Klikk på ⚙ -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Grensesnitt**.
4. I seksjonen **Viser programmets status i varslingsområdet**, velger du status og krysser av i boksen.

   Når programmet bytter til en tilstand som tilsvarer den valgte statusen, endres programikonet i varslingsområdet.

Slik passordbeskytter du tilgangen til styringsfunksjonene i programmet

En datamaskin brukes ofte av flere brukere med forskjellige datakunnskapsnivåer. Hvis ulike brukere har ubegrenset tilgang til programmet og programmets innstillinger, kan det påvirke sikkerheten til datamaskinen.

Du kan definere et administratorpassord for `KLAdmin-` kontoen for å begrense tilgangen til programmet. Denne brukeren har ubegrensede rettigheter til å administrere og endre innstillingene til programmet, og til å tilordne tilgangstillatelser for programmet til andre brukere. Når du har opprettet et passord for `KLAdmin`, kan du tilordne tilgangstillatelser for programmer til forskjellige brukere eller brukergrupper.

Slik oppretter du et administratorpassord for `KLAdmin`:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Innstillinger for grensesnitt**.
4. Sett vekslebryteren **Passordbeskyttelse** til **På**.
5. Fyll ut feltene **Brukernavn** (KLAdmin anbefales), **Skriv inn passord** og **Bekreft passord** i vinduet som åpnes.
   Tips for å lage et sterkt passord:
   - Passordet må inneholde minst 8 og ikke mer enn 128 tegn.
   - Passordet må inneholde minst ett siffer.
   - Passordet må inneholde både små og store bokstaver.
   - Passordet må inneholde minst ett spesialtegn (for eksempel: ! @ # $ % ^ & *).
6. Klikk på **Lagre**.

Du kan ikke gjenopprette et passord. Hvis du glemmer passordet ditt, må du kontakte teknisk støtte for å gjenopprette tilgangen til innstillingene for programmet.

Brukeren `KLAdmin` kan tilordne tillatelser til følgene brukere og grupper:

- Brukergruppen `Alle`. Gruppen inkluderer alle brukere i operativsystemet. Hvis du gir denne gruppetillatelsen for å utføre en bestemt handling, vil brukere i gruppen alltid ha tillatelse til å utføre handlingen, selv om en spesifikk bruker eller brukergruppe som tilhører brukergruppen `Alle` ikke har en egen tillatelse til å utføre handlingen. Som standard har brukere av gruppen `Alle` ikke tillatelser til å utføre noen handlinger.
- `<systembruker>`. Som standard har den valgte brukeren ikke tillatelse til å utføre noen handlinger. Dette betyr at når du prøver å utføre en handling som ikke er tillatt, vil du bli bedt om å angi passordet for `KLAdmin-` kontoen.

Slik legger du til en bruker eller brukergruppe:

1. Klikk på **Legg til** i delen **Innstillinger for grensesnitt** i blokken **Viser programmets status i varslingsområdet**.

   Vinduet **Legg til tillatelser for en bruker eller gruppe** vil da åpne.

2. Klikk på **Velg bruker eller gruppe** for å åpne vinduet for valg av bruker eller brukergruppe for operativsystemet.

3. I inntastingsfeltet for objektnavn angir du navnet til brukeren eller brukergruppen (for eksempel `Administrator`).

4. Klikk på **OK**.

5. I vinduet **Legg til tillatelser for en bruker eller gruppe** velg du alternativene ved siden av handlingene du ønsker å tillate for denne bestemte brukeren eller brukergruppen i blokken **Tillatelser**.

Slik redigerer du tillatelser for en bruker eller brukergruppe

I delen **Innstillinger for grensesnitt** velger du brukeren eller brukergruppen i listen i blokken **Viser programmets status i varslingsområdet** og klikker på **Rediger**.

Slik tillater du en handling for en individuell bruker eller brukergruppe

1. Åpne vinduet **Legg til tillatelser for en bruker eller gruppe** for gruppen `Alle` og fjern merket i alternativet som tillater denne handlingen hvis den er aktivert.

2. Åpne vinduet **Legg til tillatelser for en bruker eller gruppe** for den valgte brukeren og kryss av i alternativet som tillater denne handlingen.

Slik forbyr du en handling for en individuell bruker eller brukergruppe

1. Åpne vinduet **Legg til tillatelser for en bruker eller gruppe** for gruppen `Alle` og fjern merket i alternativet som tillater denne handlingen hvis den er aktivert.

2. Åpne vinduet **Legg til tillatelser for en bruker eller gruppe** for den valgte brukeren, og fjern merket i alternativet som tillater denne handlingen.

Når du prøver å utføre en handling fra listen i vinduet **Legg til tillatelser for en bruker eller gruppe**, vil programmet be deg om å skrive inn et passord. I passordvinduet skriver du inn brukernavn og passord for gjeldende brukerkonto. Denne handlingen vil bli utført hvis den spesifiserte kontoen har tillatelse til det. I passordvinduet kan du spesifisere tidsintervallet der brukeren ikke trenger å skrive inn passordet på nytt.

I passordvinduet kan du bytte inntastingsspråk kun ved å trykke på **ALT+SHIFT**. Eventuelle andre snarveier vil ikke bytte inndataspråk, selv om de er konfigurert i operativsystemet.

Slik gjenoppretter du standardinnstillinger for programmet

Du kan når som helst gjenopprette programinnstillingene som anbefales av Kaspersky. Når innstillingene er gjenopprettet, brukes **Optimalt** sikkerhetsnivå for alle beskyttelseskomponenter.

Slik gjenoppretter du standardinnstillingene for programmet:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Administrer innstillinger**.
4. Klikk på lenken **Gjenopprett** for å kjøre veiviseren for gjenoppretting av innstillinger.
5. Klikk på **Neste**.

   Vinduet for veiviseren viser fremdriften for gjenoppretting av programinnstillingene tilbake til standardinnstillingene konfigurert av Kasperskys eksperter.
6. Når standardprosessen for gjenoppretting av programinnstillinger er ferdig, klikker du på **Fullført**.

Slik bruker du programinnstillingene på en annen datamaskin

Etter å ha konfigurert Kaspersky på en bestemt måte, kan du bruke innstillingene på en annen datamaskin. Dermed vil Kaspersky være konfigurert likt på begge datamaskinene.

Innstillingene for Kaspersky-programmet lagres i en konfigurasjonsfil du kan flytte fra en datamaskin til en annen.

Innstillingene for Kaspersky-programmet kan flyttes fra en datamaskin til en annen med tre enkle trinn:

1. Lagre innstillingene for Kaspersky-programmet i en konfigurasjonsfil.
2. Overfør konfigurasjonsfilen til den andre datamaskinen (for eksempel via e-post eller ved hjelp av en flyttbar stasjon).
3. Importer innstillingene fra konfigurasjonsfilen til kopien av Kaspersky-programmet som er installert på den andre datamaskinen.

Slik eksporterer du innstillinger

Slik eksporterer du innstillinger for Kaspersky:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. I **Innstillinger**-vinduet velger du delen **Administrer innstillinger**.
4. Velg **Eksporter**.
5. Vinduet **Lagre** åpnes.
6. Angi et navn på konfigurasjonsfilen og klikk på **Lagre**.

   Programinnstillingene er nå lagret i konfigurasjonsfilen.

Du kan også eksportere innstillingene for Kaspersky-programmet på kommandolinjen ved hjelp av følgende kommando: `avp.com EXPORT <filnavn>`.

Under eksport av innstillingene for Kaspersky-programmet blir nettadresser du har lagt til i Safe Money bare lagret for gjeldende bruker. Under import av innstillinger på en annen datamaskin, blir nettadresser ikke lagret.

Slik importerer du innstillinger

Slik importerer du innstillinger til Kaspersky-programmet som er installert på en annen datamaskin:

1. Åpne hovedvinduet for Kaspersky-programmet på den andre datamaskinen.
2. Klikk på -knappen nederst i vinduet.
   Vinduet **Innstillinger** vil da åpne.
3. I **Innstillinger**-vinduet velger du delen **Administrer innstillinger**.
4. Velg **Importer**.
   Vinduet **Åpne** åpnes.
5. Angi konfigurasjonsfilen og klikk på **Åpne**.

   Innstillingene importeres til Kaspersky-programmet som er installert på den andre datamaskinen.

Slik stopper du beskyttelsen av datamaskinen midlertidig og starter den igjen

Midlertidig stopping av beskyttelse innebærer at du midlertidig deaktiverer alle beskyttelseskomponenter i en viss tid.

Når beskyttelsen stanses midlertidig eller når Kaspersky-programmet ikke kjører, overvåkes aktiviteten til programmer som kjører på datamaskinen. Informasjon om resultatene ved overvåking av programaktiviteter lagres i operativsystemet. Når Kaspersky-programmet startes på nytt eller når beskyttelsen gjenopptas, bruker programmet denne informasjonen til å beskytte datamaskinen mot skadelige handlinger som kan ha blitt utført da beskyttelsen var stanset midlertidig eller Kaspersky-programmet ikke kjørte. Informasjon om resultatene ved overvåking av programaktiviteter lagres permanent. Denne informasjonen slettes hvis Kaspersky-programmet fjernes fra datamaskinen.

Slik stopper du datamaskinbeskyttelsen midlertidig:

1. Fra hurtigmenyen til Kaspersky-ikonet i systemstatusfeltet velger du **Stopp beskyttelsen midlertidig**.

   Vinduet **Stopp beskyttelsen midlertidig** åpnes.

2. I vinduet **Stopp beskyttelsen midlertidig** velger du tidsperioden som skal forløpe før beskyttelsen startes igjen:

   - **Stopp midlertidig i** – beskyttelse aktiveres ved utløp av tidsintervallet som velges fra rullegardinlisten.
   - **Avbryt til programmet startes på nytt** – beskyttelse aktiveres når programmet startes igjen eller operativsystemet startes på nytt (hvis programmet automatisk starter ved oppstart).
   - **Stans midlertidig** – Beskyttelsen aktiveres igjen når du bestemmer deg for å gjenoppta den.

3. Klikk på **Stopp beskyttelsen midlertidig** og bekreft valget i vinduet som åpnes.

Slik gjenopptar du datamaskinbeskyttelsen

Hvis du vil gjenoppta datamaskinbeskyttelsen:

Velg **Gjenoppta beskyttelse** i hurtigmenyen til Kaspersky-ikonet i systemstatusfeltet.

Evaluere Kaspersky-programmet

Du kan evaluere programmet og sende karakteren din til Kaspersky.

En stund etter installasjonen vil programmet be deg om å evaluere hvor godt det fungerer.

For å evaluere programmet:

1. I vinduet **Vi verdsetter synspunktene dine** gjør du ett av følgende:

   - Hvis du er klar til å evaluere Kaspersky, bruker du 10-punktsskalaen til å gi en karakter.

- Hvis du ikke ønsker å evaluere programmet, klikker du på knappen × for å lukke evalueringsvinduet.

2. Klikk på knappen **Send**.
3. Klikk på **Lukk**-knappen for å lukke vinduet.

Hvilke data som overføres ved vurdering av programmet

I tillegg til vurderingen behandler Kaspersky følgende informasjon for å kunne analysere undersøkelsen:

- Navnet og versjonen til Kaspersky-programmet
- Versjonen til operativsystemet
- Området Kaspersky-programmet aktiveres i, og språket for brukergrensesnittet
- Bruksperiode for Kaspersky-programmet

Sikkerhet

Dagens hackere blir smartere når det gjelder å bryte seg inn på enhetene dine. Nye løsepengevirus, phishing og andre typer skadelig programvare krever nye cybersikkerhetsløsninger for å ligge et skritt foran de økende truslene. Vi opprettet det nye Kaspersky-programmet for å hjelpe deg med å ligge i forkant av dagens trusler. Finn ut hva du kan gjøre for å føle deg trygg.

Skanne datamaskinen

Under skanning søker programmet etter infiserte filer og skadelig programvare. Flere typer skanninger varierer når det gjelder søkets varighet og omfang.

- Fullstendig skann. Et Fullstendig skann gjennomsøker alle områdene på datamaskinen. Denne skanningen tar lang tid.
- Hurtigskann. Hurtigskann skanner objekter som lastes inn når operativsystemet starter, samt systemminne og oppstartsfiler. Denne skanningen tar ikke lang tid.
- Selektivt skann. Selektivt skann skanner den valgte filen eller mappen.
- Skanning av flyttbar stasjon. Skanning av flyttbare stasjoner som harddisker og USB-minne som er koblet til datamaskinen.
- Umiddelbar filskanning. Dette alternativet skanner filer fra hurtigmenyen.
- Bakgrunnsskanning Skanning av systemminne, systempartisjon, bootsektorer og oppstartsobjekter, samt rootkit-søk.
- Sårbarhetsskanning av programmer Skanner datamaskinen etter sårbarheter i programmer som skadelig programvare kan utnytte for å infisere systemet ditt.

Når du har installert programmet, anbefaler vi at du kjører en fullstendig skanning av datamaskinen.

Slik kjører du et Hurtigskann

Programmet skanner som standard følgende objekter under et Hurtigskann:

- Objekter som lastes ved oppstart av operativsystemet
- Systemminne
- Oppstartssektorer

Slik kjører du et Hurtigskann:

1. Åpne hovedvinduet for programmet og utfør følgende handlinger:
    - Gå til delen **Hjem** og klikk på **Hurtigskann**.

- Gå til delen **Sikkerhet**.

    1. I blokken **Skann** klikker du på **Velg skanning**-knappen.
    2. Vinduet **Skann** vil da åpne.
    3. I **Skann**-vinduet velger du delen **Hurtigskann**.
    4. I delen **Hurtigskann** klikker du på **Kjør skann**-knappen.

Programmet starter en hurtigskanning av datamaskinen.

Slik kjører du et Fullstendig skann

Programmet skanner som standard følgende objekter under et Fullstendig skann:

- Systemminne
- Objekter lastet ved oppstart av operativsystemet
- Systemets sikkerhetskopilager
- Harddisker og flyttbare stasjoner

Vi anbefaler at du kjører en fullstendig skanning umiddelbart etter at du har installert programmet på datamaskinen.

Slik kjører du et Fullstendig skann:

1. Åpne hovedvinduet for programmet og gå til delen **Sikkerhet**.
2. I blokken **Skann** klikker du på **Velg skanning**-knappen.
   Vinduet **Skann** vil da åpne.
3. I **Skann**-vinduet velger du delen **Fullstendig skann**.
4. I rullegardinlisten ved siden av **Kjør skann** velger du handlingen som skal utføres når skanningen er fullført.
5. Klikk på **Kjør skann**.

Programmet starter et Fullstendig skann av datamaskinen.

Slik kjører du et Egendefinert skann

Med et Selektivt skann kan du skanne filer, mapper eller stasjoner etter virus og andre trusler.

Slik kjører du et Egendefinert skann:

1. Åpne hovedvinduet.

2. Gå til delen **Sikkerhet**.
3. I blokken **Skann** klikker du på **Velg skanning**-knappen.
   Vinduet **Skann** vil da åpne.
4. I **Skann**-vinduet velger du delen **Selektiv skann**.
5. Klikk på knappen **Velg** og angi et objekt i vinduet for valg av fil eller mappe som åpnes.
6. Klikk på **Kjør skann**.

Slik kjører du skanning av flyttbare stasjoner

Flyttbare enheter du kobler til datamaskinen, kan inneholde virus eller andre programmer som utgjør en trussel. Kaspersky-programmet skanner flyttbare stasjoner for å forhindre at datamaskinen blir infisert. Du kan konfigurere skanning av flyttbare enheter for manuell eller automatisk start når en flyttbar enhet kobles til datamaskinen. Automatisk skanning av flyttbare enheter er aktivert som standard.

Slik kjører du Skanning av flyttbare stasjoner manuelt:

1. Åpne hovedvinduet.
2. Gå til delen **Sikkerhet**.
3. I blokken **Skann** klikker du på **Velg skanning**-knappen.
   Vinduet **Skann** vil da åpne.
4. I **Skann**-vinduet velger du delen **Skanning av flyttbar stasjon**.
5. I rullegardinlisten velger du stasjonsbokstaven til den eksterne enheten og klikker på knappen **Kjør skann**.

Programmet starter skanningen av den tilkoblede enheten.

Slik kjører du et skann av en fil eller mappe fra hurtigmenyen

Slik kjører du et skann av en fil eller mappe fra hurtigmenyen:

1. Høyreklikk på filen eller mappen som skal skannes.
2. Velg **Skann etter virus** i hurtigmenyen som åpnes.

Programmet begynner å skanne den valgte filen eller mappen.

I Microsoft Windows 11 må du utvide hurtigmenyen til et objekt for å se programkommandoene.

Aktivere eller deaktivere bakgrunnsskanning

Bakgrunnsskanning er en automatisk skannemodus i Kaspersky Total Security som ikke viser varsler. Denne skanningen bruker færre datamaskinressurser enn andre typer skanninger (for eksempel Fullstendig skanning). I denne modusen skanner programmet systemminnet, systemvolumer, bootsektorer og oppstartsobjekter, og søker etter rootkits.

En bakgrunnsskanning startes i følgende tilfeller:

- Etter at databasene og programmodulene er oppdatert
- 30 minutter etter at programmet er startet
- Hver sjette time
- Hvis datamaskinen forblir inaktiv i fem minutter eller mer (etter at skjermspareren er aktiv)

En bakgrunnsskanning avbrytes når noen av følgende betingelser er oppfylt:

- Datamaskinen er i bruk igjen.
- Datamaskinen (bærbar PC) bytter til batterimodus.

Hvis det ikke har blitt kjørt en bakgrunnsskanning på over ti dager, stoppes ikke skanningen. Når du kjører en bakgrunnsskanning, skanner ikke programmet filer som har innhold på skylagringssystemet OneDrive.

Aktivere eller deaktivere en bakgrunnsskanning:

1. Åpne hovedvinduet.
2. Gå til delen **Sikkerhet**.
3. I blokken **Skann** klikker du på **Velg skanning**-knappen.
   Vinduet **Skann** vil da åpne.
4. Klikk på -ikonet i blokken **Bakgrunnssøk**.
   Vinduet **Innstillinger for Bakgrunnssøk** vil da åpne.
5. I vinduet **Innstillinger for Bakgrunnssøk** endrer du bryteren til **På** eller **Av**.

Slik oppretter du en skannetidsplan

Slik oppretter du en skannetidsplan:

1. Åpne hovedvinduet.
2. Gå til delen **Sikkerhet**.
3. I blokken **Skann** klikker du på **Velg skanning**-knappen.
   Vinduet **Skann** vil da åpne.

4. I vinduet **Skann** velger du typen skanning og klikker på -ikonet.

5. I vinduet som åpnes klikker du på **Skannetidsplan** for å gå videre til vinduet **Skannetidsplan**.

6. I vinduet **Skannetidsplan** velger du en periode i listen **Kjør skann**, for eksempel **Hver dag**, og spesifiserer tidspunktet for å starte skanningen.

Det kan ikke opprettes en skannetidsplan for et skann fra hurtigmenyen eller Bakgrunnsskanning.

Slik søker du etter sårbarheter i programmer installert på datamaskinen din

Programmer som er installert på datamaskinen, kan ha sårbarheter som kan utnyttes av skadelig programvare. Skanning av datamaskinen vil hjelpe deg med å finne disse sårbarhetene og hindre at datamaskinen din blir infisert.

Slik kjører du Sårbarhetsskanning av programmer:

1. Åpne hovedvinduet.

2. Gå til delen **Sikkerhet**.

3. I blokken **Skann** klikker du på **Velg skanning**-knappen.
   Vinduet **Skann** vil da åpne.

4. I **Skann**-vinduet velger du delen **Sårbarhetsskanning av programmer**.

5. Klikk på **Kjør skann**.

Programmet begynner å skanne datamaskinen for sårbarheter i programmer.

Slik ekskluderer du en fil, mappe eller trusseltype fra skanning

Slik ekskluderer du en fil, mappe eller trusseltype fra skanning:

1. Åpne hovedvinduet.

2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.

3. Gå til **Sikkerhetsinnstillinger** → **Trusler og unntak**.

4. Klikk på **Behandle unntak** for å åpne vinduet **Unntak**.

5. Klikk på **Legg til**.

6. Legg til et unntak på en av følgende måter:

   - Klikk på **Bla gjennom** og velg mappen eller filen du vil ekskludere fra skanning. Klikk på **Velg**.

- I feltet **Fil eller mappe** skriver du inn hele navnet eller masken til filen eller mappen.
- I feltet **Objekt** skriver du inn hele navnet eller masken til trusseltypen i henhold til Kaspersky-klassifiseringen for det oppdagede objektet.
- Hvis du fyller ut både **Fil eller mappe** og **Objekt**, skannes ikke den angitte filen eller mappen for den angitte trusseltypen.
- I feltet **Fil-hash** angir du hash-koden hvis du vil at filer ikke skal skannes etter hash-koden.

7. Fjern avmerkingsboksene for beskyttelseskomponenter som unntaksregelen ikke skal gjelde for. Skriv inn en kommentar om du vil.
8. Velg **Aktiv**-status for regelen og klikk på **Legg til**.

De angitte objektene ekskluderes fra skanning.

Ytterligere informasjon om innstillinger i vinduet Trusler og unntak

Skanning av filer i skylageret OneDrive

I Windows 10 RS3 og nyere versjoner vil programmet ikke skanne filer i skylageret OneDrive. Hvis programmet oppdager slike filer under en skanning, viser det et varsel om at filene i skylageret ikke ble skannet.

Følgende komponenter skanner ikke filer i skylageret OneDrive:

- Fullstendig skann
- Selektivt skann
- Hurtigskann
- Bakgrunnsskanning

Rapporten om operasjonene til programmet inneholder en liste med filer i OneDrive-skylageret som ble hoppet over under skanning.

Filer lastet ned fra skylageret OneDrive til en lokal datamaskin skannes av sanntids beskyttelseskomponenter. Hvis skanning av en fil ble utsatt, og filen har blitt lastet opp igjen til skylageret OneDrive før skanningen startes, kan det hende denne filen hoppes over under en skanning.

Når programmer og skript kjøres, vil komponentene Inntrengningsbeskyttelse og Systemvakt laste ned programmer fra OneDrive-skylageret til den lokale datamaskinen for å skanne dem.

For å sikre at OneDrive-filer vises i Utforsker må du slå på funksjonen Filer på etterspørsel i klientprogrammet OneDrive. Hvis du er tilkoblet Internett, kan du bruke dem akkurat som alle andre filer på datamaskinen din.

Oppdatere antivirusdatabaser og programmoduler

Denne delen inneholder informasjon om oppdatering av databaser og programmoduler.

Om oppdatering av databaser og programmoduler

Installasjonspakken til programmet inneholder også databaser og programmoduler. Bruk av disse databasene:

- Programmet oppdager mesteparten av truslene ved hjelp av Kaspersky Security Network, som krever Internett-tilkobling.
- Programmet oppdager annonseprogrammer, oppringningsprogrammer og annen lovlig programvare som kriminelle kan bruke til å skade datamaskinen eller de personlige dataene dine.

Vi anbefaler at du oppdaterer antivirusdatabasene og programmodulene så snart programmet er installert, for å få full beskyttelse.

Databaser og programmoduler oppdateres trinnvis:

1. Programmet starter oppdatering av databaser og programmoduler i henhold til angitte innstillinger: automatisk, etter en tidsplan eller på forespørsel. Programmet kontakter en oppdateringskilde som lagrer en oppdateringspakke for antivirusdatabaser og programmoduler.
2. Programmet sammenligner de eksisterende databasene med databasene som er tilgjengelige på oppdateringskilden. Hvis databasene er forskjellige, laster programmet ned de manglende elementene i databasene.

Programmet bruker deretter de oppdaterte databasene og programmodulene til å skanne datamaskinen etter virus og andre trusler.

Oppdateringskilder

Du kan bruke følgende oppdateringskilder:

- Kasperskys oppdateringsservere
- HTTP- eller FTP-server
- Nettverksmappe

Spesielle hensyn ved oppdatering av antivirusdatabaser og programmoduler

Oppdatering av antivirusdatabaser og programmoduler er underlagt følgende begrensninger og vilkår:

- Antivirusdatabaser anses som utdaterte etter en dag og fullstendig utdaterte etter syv dager.
- Du må ha Internett-tilkobling for å kunne laste ned en oppdateringspakke fra Kasperskys servere.
- Oppdatering av antivirusdatabaser og programmoduler er ikke tilgjengelig i følgende situasjoner:
  - Abonnementet har utløpt, og gratisperioden eller modus for begrenset funksjonalitet er ikke tilgjengelig.
  - Du bruker en tariffbasert mobil Internett-tilkobling. Denne begrensningen gjelder for datamaskiner som kjører Microsoft Windows 8 eller nyere versjoner av dette operativsystemet, dersom automatisk oppdatering eller tidsplanlagt oppdatering er aktivert, og det er angitt en trafikkgrense for en tariffbasert

mobiltilkobling. Hvis du vil at programmet skal oppdatere antivirusdatabaser og programmoduler i slike tilfeller, må du deaktivere alternativet **Begrens trafikk på kostnadspliktige tilkoblinger** i **Innstillinger** → **Sikkerhetsinnstillinger** → **Avanserte innstillinger** → **Nettverksinnstillinger**.

- Programmet brukes under et abonnement fra en tjenesteleverandør, og du har suspendert abonnementet på nettstedet til tjenesteleverandøren.

Installere en oppdateringspakke

Når en oppdateringspakke (korrigering) mottas, installerer programmet den automatisk. Du må starte datamaskinen på nytt for å fullføre installasjonen av en oppdateringspakke. Frem til datamaskinen startes på nytt, er programikonet i oppgavelinjen rødt mens vinduet **Varslingssenter** i programmet viser en melding som ber deg om å starte datamaskinen på nytt.

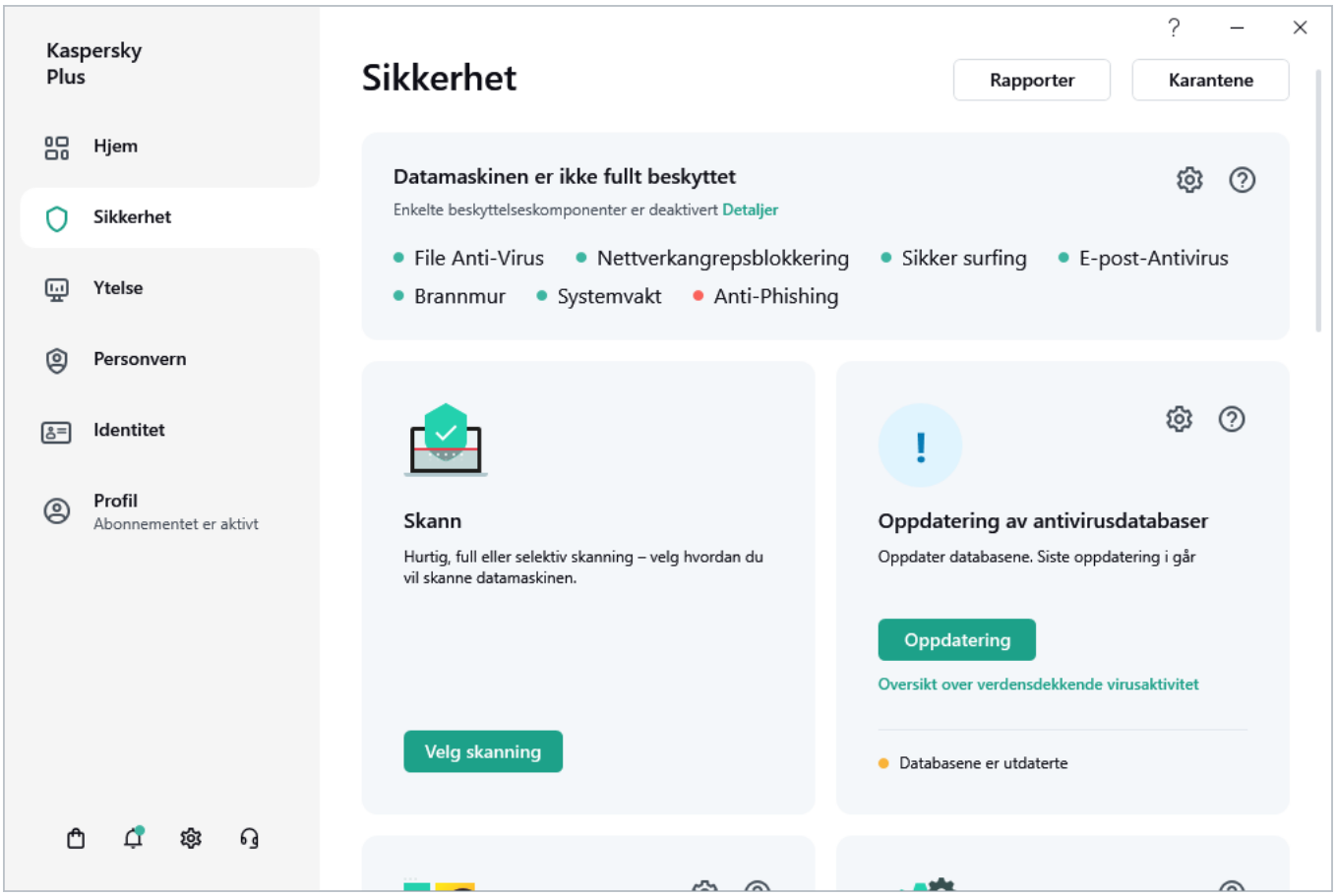
Slik starter du en oppdatering av databaser og programmoduler

Som standard oppdateres databaser og programmoduler automatisk. Du trenger ikke gjøre noe. Hvis automatiske oppdateringer er deaktivert, kan du oppdatere programdatabaser og moduler manuelt.

Slik starter du en oppdatering av databaser og programmoduler:

1. Åpne hovedvinduet.
2. Gå til delen **Sikkerhet**.
3. I blokken **Oppdatering av antivirusdatabaser** klikker du på **Oppdater**-knappen.

Antivirus database oppdatering



Inntrengningsbeskyttelse

Kaspersky-programmet bidrar til å minimere risikoen ved bruk av ukjente programmer (for eksempel risikoen for å bli infisert av virus og annen skadelig programvare).

Kaspersky-programmet inneholder komponenter og verktøy som kan brukes til å sjekke programmets omdømme og kontrollere aktiviteter som utføres på datamaskinen.

Om Inntrengningsbeskyttelse

Kun tilgjengelig i Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Komponenten Inntrengningsbeskyttelse forhindrer at programmer utfører handlinger som kan være farlig for operativsystemet, og sikrer kontroll av tilgang til operativsystemets ressurser (inkludert filressurser på eksterne datamaskiner) og personopplysningene dine.

Inntrengningsbeskyttelse sporer handlinger i operativsystemet, som er utført av programmer installert på datamaskinen, og regulerer dem basert på definerte regler. Disse reglene begrenser potensielt farlig programaktivitet, inkludert programmers tilgang til beskyttede ressurser, som f.eks. filer, mapper, registreringsnøkler og nettverksadresser.

På 64-biters operativsystemer kan ikke programmenes rettigheter for følgende handlinger konfigureres:

- Direkte tilgang til fysisk minne

- Behandle skriverdrivere
- Opprettelse av tjenester
- Lesing av tjenester
- Redigering av tjenester
- Omkonfigurering av tjenester
- Behandling av tjenester
- Start av tjenester
- Fjerning av tjenester
- Tilgang til interne nettleserdata
- Tilgang til kritiske objekter i operativsystemet
- Tilgang til passordlager
- Angi feilsøkingsrettigheter
- Bruk av programgrensesnittene i operativsystemet
- Bruk av programgrensesnittene i operativsystemet (DNS)
- Bruk av programgrensesnitt for andre programmer
- Endre systemmoduler (KnownDlls)
- Starte drivere

På 64-biters Microsoft Windows 8 og Microsoft Windows 10 kan ikke programmenes rettigheter for følgende handlinger konfigureres:

- Sende vindusmeldinger til andre prosesser
- Mistenkelige operasjoner
- Installering av tastelogger
- Avbrudd i innkommende dataflythendelser
- Muligheten til å ta skjermbilder

Programmenes nettverksaktivitet kontrolleres av Brannmur-komponenten.

Når et program startes på datamaskinen for første gang, kontrollerer Inntrengningsbeskyttelse sikkerheten til programmet, og tilordner det til en gruppe (Klarert, Uklarert, Høyt begrenset eller Lavt begrenset). Klareringsgruppen definerer reglene som Kaspersky skal bruke til å kontrollere aktivitetene til dette programmet.

Kaspersky-programmet tilordner programmene til klareringsgrupper (Klarert, Uklarert, Høyt begrenset eller Lavt begrenset), men kun hvis Inntrengningsbeskyttelse eller Brannmur er aktivert, eller hvis begge disse komponentene er aktivert. Hvis begge komponentene er deaktivert, fungerer ikke funksjonen som tilordner programmene til klareringsgrupper.

Du kan redigere reglene for programkontroll manuelt.

Reglene du velger for programmer arves av underordnede programmer. Hvis du for eksempel nekter all nettverksaktivitet for cmd.exe, vil disse aktivitetene også bli nektet for notepad.exe når programmet startes ved hjelp av cmd.exe. Når et program ikke er en underordnet del av programmet den kjører fra, arves ikke reglene.

Slik endrer du innstillinger for Inntrengningsbeskyttelse

Kun tilgjengelig i Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Slik endrer du innstillinger for Inntrengningsbeskyttelse:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Sikkerhetsinnstillinger**.
4. Aktiver komponenten **Inntrengningsbeskyttelse**.
5. I vinduet **Innstillinger for Inntrengningsbeskyttelse** klikker du på lenken **Behandle programmer** for å åpne vinduet **Behandle programmer**.
6. Velg programmet du trenger i listen, og dobbeltklikk på navnet for å åpne vinduet **Programregler**.
7. Slik konfigurerer du reglene for et programs tilgang til ressurser i operativsystemet:
   a. I kategorien **Filer og systemregister** velger du ønsket ressurskategori.
   b. Klikk på ikonet i kolonnen med en tilgjengelig handling for ressursen (**Les**, **Skriv**, **Slett** eller **Opprett**) for å åpne menyen. I menyen velger du det aktuelle elementet (**Arv**, **Tillat**, **Spør brukeren** eller **Nekt**).
8. Slik konfigurerer du et programs rettigheter til å utføre bestemte handlinger i operativsystemet:
   a. Velg ønsket kategori med rettigheter i kategorien **Rettigheter**.
   b. I kolonnen **Handling** klikker du på ikonet for å åpne menyen og velger det aktuelle elementet (**Arv**, **Tillat**, **Spør brukeren** eller **Nekt**).
9. Slik konfigurerer du et programs rettigheter til å utføre bestemte handlinger i nettverket:
   a. I kategorien **Nettverksregler** klikker du på **Legg til**.
   Vinduet **Nettverksregel** vil da åpne.
   b. I vinduet som åpnes, angir du ønskede regelinnstillinger og klikker på **Lagre**.
   c. Tilordne en prioritet til den nye regelen. Det gjør du ved å velge regelen og flytte den opp eller ned i listen.

10. Hvis du vil utelate bestemte programhandlinger fra begrensningene skanning, går du til kategorien **Unntak** og merker av for handlinger som ikke skal kontrolleres.

11. Klikk på **Lagre**.

    Alle unntak som er opprettet i Regler for Inntrengningsbeskyttelse, er tilgjengelige i vinduet med innstillinger for Kaspersky-programmet, under delen **Trusler og unntak**.

Inntrengningsbeskyttelse overvåker og begrenser handlingene til programmet i samsvar med de spesifiserte innstillingene.

Sjekke programmets omdømme

Med Kaspersky kan du lære omdømmet til programmer fra brukere over hele verden. Et programs omdømme omfatter følgende kriterier:

- Navn på leverandør
- Informasjon om den digitale signaturen (hvis programmet er digitalt signert)
- Informasjon om gruppen programmet er tilordnet av Inntrengningsbeskyttelse eller størstedelen av Kaspersky Security Network-brukerne
- Antallet brukere av Kaspersky Security Network som anvender programmet (tilgjengelig hvis programmet har blitt inkludert i gruppen Klarert i Kaspersky Security Network-databasen)
- Tidspunktet for når programmet ble kjent i Kaspersky Security Network
- Land hvor programmet er mest utbredt

Sjekking av programmets omdømme er tilgjengelig hvis du har godtatt å delta i Kaspersky Security Network.

Hvis du vil vite mer om omdømmet til et program:

Åpne hurtigmenyen til programmets kjørbare fil og velg **Kontroller omdømme i KSN**.

Et vindu med informasjon om programmets omdømme i Kaspersky Security Network åpnes.

Skann for svake innstillinger

I denne delen vil du lære om svake innstillinger i operativsystemet, og om hvordan du kan søke etter og reparere svake innstillinger i operativsystemet.

Om svake innstillinger i operativsystemet

Når du jobber med en datamaskin, kan operativsystemets innstillinger endres over tid, enten pga. handlingene dine, eller handlingene til programmer du bruker. Hvis du endrer innstillingene av operativsystemet, kan du sette datamaskinens sikkerhet i fare. Hvis for eksempel automatisk pålogging med brukernavn og passord er aktivert i Internet Explorer, kan et tredjepartsnettsted fange opp passordet ditt.

Svake innstillinger i operativsystemet kan deles inn i to typer:

- *Kritiske innstillinger*. Slike innstillinger tilsvarer sårbarheter i operativsystemet.
- *Anbefalte innstillinger*. Vi anbefaler at du reparerer disse innstillingene for å øke sikkerheten til operativsystemet.

Som standard skanner programmet etter svake innstillinger i operativsystemet minst én gang om dagen. Hvis programmet oppdager svake innstillinger i operativsystemet, blir du bedt om å reparere dem for å gjenopprette operativsystemets sikkerhet. For detaljer om hver svak innstilling, klikk på koblingen ved siden av den relevante innstillingen i programvinduet.

Du kan klikke på koblingen i varslingsvinduet for å gå til vinduet **Skanning av svake innstillinger**, som viser de svake innstillingene som ble oppdaget i operativsystemet. Informasjon om svake innstillinger vises også i Varslingssenter. Du kan vise og reparere de svake innstillingene fra Varslingssenter.

I vinduet **Skanning av svake innstillinger** kan du utføre følgende handlinger:

- Reparere svake innstillinger i operativsystemet.
- Ignorer: La svake innstillinger i operativsystemet forbli uendret.
- Avbryt: Gjenopprett svake innstillinger du allerede har reparert i operativsystemet, til opprinnelig tilstand.

Programmet identifiserer svake innstillinger i operativsystemet for alle brukerkontoer på datamaskinen. Du kan reparere svake innstillinger for andre brukerkontoer på datamaskinen, men dette er kun mulig hvis du har logget på operativsystemet med en administratorkonto.

> Hvis du ikke er administrator av datamaskinen, kan du bare ignorere svake innstillinger for din egen brukerkonto. Bare en datamaskinadministrator kan ignorere svake innstillinger for alle brukerkontoer.

Du kan starte en skanning etter svake innstillinger manuelt, eller deaktivere skannning etter svake innstillinger.

Du kan fjernstyre datamaskinens beskyttelse og sende en kommando om å reparere svake innstillinger fra My Kaspersky.

Slik finner og reparerer du svake innstillinger i operativsystemet

Slik skanner du etter og reparerer svake innstillinger i operativsystemet:

1. Åpne hovedvinduet.
2. Velg delen **Sikkerhet**.
3. Under **Sikkerhet** velger du **Skanning av svake innstillinger**.
4. Klikk på **Skann**.

   Dette kjører et skann for svake innstillinger. Etter at skanningen er fullført, ser du resultatene av skanningen i delen **Skanning av svake innstillinger**.

5. Klikk på **Vis** for å gå til vinduet **Skanning av svake innstillinger**.

6. I vinduet **Skanning av svake innstillinger** velger du handlingen som skal utføres på svake innstillinger:

   - Oppdaget svake innstillinger. Gjør ett av følgende:

     - Klikk på **Reparer alle** for å reparere alle svake innstillinger.

     - Klikk på **Reparer** for å reparere en svak innstilling.

     - Hvis åpne programmer forstyrrer rettingen av en svak innstilling, klikker du på **Vis** for å vise listen over forstyrrende programmer.

       For å lukke programmer som hindrer at innstillingen rettes, gjør du ett av følgende:

       - Klikk på ✕ til høyre for navnet på det forstyrrende programmet for å lukke det på vanlig måte. Hvis programmet oppdager ulagrede endringer, vil det be deg om å lagre dem.

       - Klikk på koblingen **Tving lukking** for å lukke alle forstyrrende programmer uten å lagre data.

     - I rullegardinlisten ved siden av **Reparer** velger du **Ignorer** for å å la en svak innstilling være uendret.

     - I rullegardinlisten ved siden av **Reparer** velger du **Les mer** for å se informasjon om en svak innstilling på Kasperskys nettsted for teknisk støtte.

   - Svake innstillinger som er reparert tidligere.

     - Klikk på **Rull tilbake** for å gjenopprette de reparerte innstillingen til den opprinnelige tilstanden.

     - I rullegardinlisten ved siden av **Rull tilbake** velger du **Les mer** for å se informasjon om en svak innstilling på Kasperskys nettsted for teknisk støtte.

   - Ignorerte innstillinger. Klikk på koblingen **Vis alle** ved siden av meldingen **N ignorerte innstillinger** for å åpne listen over svake innstillinger som du har latt forbli uendret, og klikk på knappen **Reparer**.

Slik aktiverer du Skann for svake innstillinger

Slik deaktiverer du Skann for svake innstillinger:

1. Åpne hovedvinduet.

2. Klikk på ⚙-knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.

3. Gå til delen **Ytelsesinnstillinger**.

4. Klikk på **PC-ressursforbruk**.

5. Deaktiver alternativet **Skanning etter svake operativsysteminnstillinger**.

Programmet vil ikke skanne etter svake innstillinger i operativsystemet eller vise varsler om dem.

Nettverksovervåker

Kun tilgjengelig i Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Med nettverksovervåker kan du se datamaskinens nettverksaktivitetsdata i sanntid, blokkere nettverksaktivitet eller lage nettverks- og pakkeregler for programmer installert på datamaskinen.

Slik går du til innstillingene for Nettverksovervåker:

1. Åpne hovedvinduet.
2. Gå til delen **Sikkerhet**.
3. I blokken **Nettverksovervåker** klikker du på **Vis**-knappen.

Vinduet **Nettverksovervåker** vil da åpne.

Delen **Nettverksaktivitet** viser alle aktive nettverkstilkoblinger. Den viser både inngående og utgående tilkoblinger. Du kan bruke lenken **Blokker all nettverksaktivitet** for å blokkere alle nettverkstilkoblinger.

Delen **Åpne porter** viser alle åpne nettverksporter. Du kan også bruke denne delen til å lage nettverks- og pakkeregler for programmer.

Delen **Nettverkstrafikk** viser mengden innkommende og utgående nettverkstrafikk mellom PC-en og andre datamaskiner på nettverket.

Delen **Blokkerte datamaskiner** inneholder en liste over IP-adresser for eksterne datamaskiner det er oppdaget forsøk på nettverksangrep fra, og som Nettverkangrepsblokkering har blokkert nettverksaktiviteten til.

Smart Home Monitor

Denne delen inneholder informasjon om hvordan du bruker Kaspersky-programmet til å finne ut hvilke enheter som er koblet til ditt Ethernet-nettverket (wireline) og det trådløse nettverket ditt.

Om komponenten Smart Home Monitor

Kun tilgjengelig i Kaspersky Plus og Kaspersky Premium.

Hackere kan potensielt få tak i passordet ditt eller hacke seg inn på hjemmenettverket ditt, enten for å bruke nettet eller for å stjele data. Kaspersky-programmet beskytter det kablede Ethernet-nettverket og trådløse nettverk mot uautoriserte tilkoblinger.

Så snart du bekrefter at hjemmenettverket ditt er oppdaget riktig, begynner vi å overvåke enheter som er koblet til dette nettverket og enkelte sårbarheter, for eksempel svak Wi-Fi-passord- eller ruterkryptering. Hvis vi oppdager sårbarheter eller en ny enhet på nettverket som du ikke har identifisert som en kjent enhet, advarer vi deg om det og foreslår anbefalinger så du kan iverksette tiltak for å beskytte hjemmenettverket ditt og enhetene som bruker det.

Varsler om sårbarheter i hjemmenettverk er bare tilgjengelig i Kaspersky Premium. Varsler om nye enheter som kobler seg på hjemmenettverket ditt, er tilgjengelig i *Kaspersky Plus og Kaspersky Premium*.

Når en enhet kobler seg på nettverket ditt, vil Kaspersky-programmet vise et varsel og spørre om du ønsker å se hvilke enheter som er koblet på dette nettverket:

- Hvis du velger Ja, vil Kaspersky-programmet vise en liste over enhetene som er koblet til dette nettverket og varsle deg hvis en ny enhet har koblet til det.
- Hvis du nekter, varsles du ikke av Kaspersky-programmet når det opprettes en tilkobling til dette nettverket i fremtiden. Listen over tilkoblede enheter vises heller ikke.

Du kan deaktivere Smart Home Monitor. Når du deaktiverer komponenten, slutter Kaspersky-programmet å varsle deg om tilkoblinger til nettverket.

Besøk nettstedet for teknisk støtte for å lese om andre tilgjengelige sikkerhetsmetoder for tilkobling til trådløse nettverk.

Slik aktiverer eller deaktiverer du Smart Home Monitor

Slik aktiverer eller deaktiverer du Smart Home Monitor:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i vinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Sikkerhetsinnstillinger**.
4. Velg komponenten Brannmur.
5. Gjør ett av følgende:
   - For å aktivere Smart Home Monitor velger du avkrysningsboksen **Vis enheter som er koblet til nettverkene mine**.
   - For å deaktivere Smart Home Monitor fjerner du merkingen i boksen **Vis enheter som er koblet til nettverkene mine**.

Slik viser du Enheter i Mitt nettverk

Kaspersky-programmet viser følgende informasjon om enheter som er koblet til det trådløse nettverket eller kablede Ethernet-nettverket ditt:

- Enhetsnavn
- Enhetens produsent

- Type enhet (f.eks. datamaskin, mobilenhet, ruter, spillkonsoll eller videokamera)
- Hvilket operativsystem som er installert på enheten
- MAC-adresse (enhetens unike nettverks-ID)
- Enhetens IP-adresse
- Klokkeslettet da frakoblede enheter sist ble oppdaget på nettverket
- Kaspersky-programmer installert på enheten din

Slik viser du enheter som er koblet til nettverket ditt:

1. Åpne hovedvinduet.
2. Gjør ett av følgende:
   - Gå til **Sikkerhet**-blokken, og klikk på **Vis**-knappen i delen **Smart Home Monitor**.
   - I hovedprogramvinduet klikker du på **Vis**-knappen i delen **Smart Home Monitor**.
   - Klikk på **<nettverksnavn>**-lenken som vises i den nedre delen av hovedvinduet.

   Vinduet **Smart Home Monitor** åpnes og viser nettverket som datamaskinen er koblet til.
3. Aktiver alternativet **Vis informasjon om enheter på dette nettverket på mobilenhetene mine** hvis du vil overføre informasjon om enheter koblet til dette nettverket til mobilenhetene dine.
4. Klikk på **Ja, vis enhetene mine** for å se enhetene som er koblet til nettverket.
   Vinduet **Smart Home Monitor** viser:
   - Enheter som for øyeblikket er koblet til nettverket ditt.
   - Enheter som var koblet til nettverket ditt for en stund siden.
   - Enhetsstatus i nettverket:
     - Tilkoblede enheter er grønne
     - Frakoblede enheter er grå
     - Nye enheter indikeres som **nye**

Slik endrer du navnet på en enhet:

1. Velg den aktuelle enheten fra listen over enheter i vinduet **Smart Home Monitor**.
   Et vindu åpnes for å vise informasjon om denne enheten.
2. Skriv inn det nye navnet på enheten i feltet **Enhetsnavn**.

Slik endrer du enhetstypen

1. Velg den aktuelle enheten fra listen over enheter i vinduet **Smart Home Monitor**.
   Et vindu åpnes for å vise informasjon om denne enheten.
2. I feltet **Enhetstype** klikker du på **Velg en type** for å gå til vinduet **Enhetstype**.
3. I det vinduet velger du enhetskategori og type, for eksempel, **Husholdningsapparater** → **Kjøleskap**).
4. Klikk på **Lagre**.

Slik nekter du nettverkstilgang for en enhet

Slik nekter du nettverkstilgang for en enhet:

1. Åpne hovedvinduet.
2. Gjør ett av følgende:
   - Gå til **Sikkerhet**-blokken, og klikk på **Vis**-knappen i delen **Smart Home Monitor**.
   - I hovedprogramvinduet klikker du på **Vis**-knappen i delen **Smart Home Monitor**.
   - Klikk på **<nettverksnavn>**-lenken som vises i den nedre delen av hovedvinduet.
3. I vinduet **Smart Home Monitor** velger du enheten du vil koble fra.
   Dette åpner et vindu med informasjon om denne enheten, inkludert informasjon om enhetens MAC-adresse.
4. Skriv ned enhetens MAC-adresse
5. Blokker enhetens MAC-adresse i nettleserinnstillingene. Besøk nettstedet til leverandøren for å se brukerhåndboken for ruteren.

Etter at MAC-adressen er blokkert, vil ikke enheten kunne koble til nettverket ditt.

Slik sletter du et nettverk uten tilkoblinger fra listen

Slik sletter du et nettverk uten tilkoblinger fra listen:

1. Åpne hovedvinduet.
2. Gjør ett av følgende:
   - Gå til **Sikkerhet**-blokken, og klikk på **Vis**-knappen i delen **Smart Home Monitor**.
   - I hovedprogramvinduet klikker du på **Vis**-knappen i delen **Smart Home Monitor**.
3. Klikk på **<nettverksnavn>**-lenken som vises i den nedre delen av hovedvinduet.

Dette tar deg til vinduet **Smart Home Monitor**.

4. Klikk på pilen i høyre del av listen for å utvide den, og klikk på ved siden av nettverket du vil fjerne.

Nettverket vil bli slettet fra listen.

Slik deaktiverer du varsler når enheter kobles til nettverket ditt

Slik deaktiverer du varslinger når enheter kobles til nettverket ditt:

1. Åpne hovedvinduet.
2. Gjør ett av følgende:
   - Gå til **Sikkerhet**-blokken, og klikk på **Vis**-knappen i delen **Smart Home Monitor**.
   - I hovedprogramvinduet klikker du på **Vis**-knappen i delen **Smart Home Monitor**.
   - Klikk på **<nettverksnavn>**-lenken som vises i den nedre delen av hovedvinduet.
3. I vinduet **Smart Home Monitor** klikker du på ••• -knappen ved siden av nettverket og velger elementet **Deaktiver varslinger**.

Kaspersky-programmet viser deg ikke lenger varsler hvis enheter kobler til dette nettverket.

Du kan også deaktivere varsler for det valgte nettverket når Kaspersky-programmet viser deg et varsel om at en enhet har koblet til dette nettverket. Det gjør du ved å klikke på koblingen **Deaktiver varslinger for dette nettverket** i varslingsvinduet.

Slik sender du tilbakemeldinger om Smart Home Monitor

Slik sender du tilbakemeldinger til Kaspersky om funksjonen til komponenten Smart Home Monitor:

1. Åpne hovedvinduet.
2. Gjør ett av følgende:
   - Gå til **Sikkerhet**-blokken, og klikk på **Vis**-knappen i delen **Smart Home Monitor**.
   - I hovedprogramvinduet klikker du på **Vis**-knappen i delen **Smart Home Monitor**.
   - Klikk på **<nettverksnavn>**-lenken som vises i den nedre delen av hovedvinduet.
3. I vinduet **Smart Home Monitor** klikker du på ••• -knappen og velger **Send tilbakemelding**.
   Vinduet **Hjelp oss med å bli bedre! Gi oss en tilbakemelding** vil da åpne.
4. Vurder komponenten på en skala fra 1 til 5 ved å velge 1 til 5 stjerner.
5. Hvis du ga en komponent 3–5 stjerner:

a. Hvis du vil legge ved en kommentar til tilbakemeldingen din, skriver du den inn i feltet **Detaljer**.

b. Velg avkrysningsboksen **Jeg aksepterer å gi dere de personlige dataene mine (unik ID for datamaskinen) for å forbedre programvaren, og jeg godtar betingelsene i personvernerklæringen**.

6. Hvis du ga en komponent 1-2 stjerner:

a. Hvis du vil varsle Kaspersky om et problem med komponenten Smart Home Monitor, velger du emnet som korresponderer best, fra rullegardinlisten **Emne**.

Du kan velge ett av følgende alternativer fra listen:

- **Upraktisk å bruke**. Velg dette elementet hvis du opplever ulemper når du bruker komponenten Smart Home Monitor.
- **Programmet bruker for lang tid til å søke etter enheter i nettverket**. Velg dette elementet hvis komponenten Smart Home Monitor jobber for sakte.
- **Programmet identifiserer enheter i nettverket feil**. Velg dette elementet hvis programmet feilaktig bestemmer navnene på og/eller typene enheter som er koblet til det trådløse nettverket eller kablede Ethernet-nettverket.
- **For mange varsler om nye enheter i nettverket**. Velg dette elementet hvis programmet viser deg for mange varsler om nye enheter i det trådløse nettverket eller kablede Ethernet-nettverket.
- **Redusert PC-ytelse**. Velg dette elementet hvis bruken av komponenten Smart Home Monitor reduserer datamaskinens ytelse.
- **Kan ikke konfigurere komponenten**. Velg dette elementet hvis du opplever problemer når du konfigurerer komponenten Smart Home Monitor.
- **Annet**. Velg dette elementet hvis problemet du opplever ikke dekkes av andre elementer.

b. Hvis du vil legge ved en kommentar til tilbakemeldingen din, skriver du den inn i feltet **Detaljer**.

c. Velg avkrysningsboksen **Jeg aksepterer å gi dere de personlige dataene mine (unik ID for datamaskinen) for å forbedre programvaren, og jeg godtar betingelsene i personvernerklæringen**.

7. Klikk på **Send**.

Når disse dataene sendes, mottar og behandler Kaspersky følgende informasjon:

- Tilbakemeldingen din, som inneholder en vurdering av komponentens ytelse, problememnet og kommentar.
- Operativsysteminformasjon og versjon.
- Informasjon om det installerte programmet og dets versjon.

Kaspersky mottar og behandler denne informasjonen i kryptert form for å analysere feil og forbedre ytelsen til komponenten Smart Home Monitor Kaspersky krever ikke at du oppgir personlig informasjon når du sender tilbakemeldinger og samler ikke inn slik informasjon. Se Kasperskys retningslinjer for personvern for mer informasjon om hvordan personopplysninger behandles.

Fjerne virus fra før Kaspersky ble tatt i bruk

Denne delen inneholder informasjon om hvordan du gjenoppretter operativsystemet etter at det har vært infisert med skadelig programvare.

Gjenopprette operativsystemet etter infisering

Hvis du mistenker at operativsystemet på datamaskinen er skadet eller endret av skadelig programvare eller på grunn av systemsvikt, bruker du *feilsøkingsveiviseren i Microsoft Windows* til å fjerne alle spor av skadelige objekter i systemet. Kaspersky anbefaler at du kjører veiviseren etter at datamaskinen er desinfisert for å sikre at alle trusler og skader forårsaket av infeksjoner har blitt fikset.

Veiviseren sjekker om det finnes endringer i systemet, for eksempel blokkering av nettverkstilgang, endringer av filtypene til kjente filformater, blokkering av Kontrollpanel osv. Slike skader kan ha forskjellige årsaker. Disse årsakene kan omfatte aktivitetene til skadelige programmer, feil systemkonfigurasjon, systemsvikt, eller til og med feil bruk av systemoptimaliseringsprogrammer.

Når gjennomgangen er fullført, analyserer veiviseren informasjonen for å vurdere om det er systemskader som krever umiddelbar oppmerksomhet. Veiviseren bruker gjennomgangen til å lage en liste over handlinger som kreves for å eliminere skaden. Veiviseren grupperer disse handlingene etter kategori basert på alvorlighetsgraden av oppdagede problemer.

Feilsøking av operativsystemet med Microsoft Windows Feilsøkingsveiviser

Slik starter du feilsøkingsveiviseren i Microsoft Windows:

1. Åpne hovedvinduet.
2. Gå til **Sikkerhet** → **Microsoft Windows Feilsøking**.
3. Klikk på **Finn skade**.

   Vinduet for feilsøkingsveiviseren i Microsoft Windows åpnes.

Veiviseren består av en rekke skjermbilder (trinn) som du kan navigere i med knappene **Tilbake** og **Neste**. Klikk på **Fullført**-knappen for å lukke veiviseren når den er fullført. Du kan når som helst stoppe veiviseren ved å klikke på **Avbryt**.

La oss gå grundigere gjennom trinnene i veiviseren.

Start gjenoppretting av operativsystemet

a. Velg ett av de to alternativene for veiviseroperasjonen:

- **Søk etter skader forårsaket av skadelig programaktivitet**. Veiviseren søker etter problemer og mulige skader.
- **Rull tilbake endringer**. Veiviseren vil rulle tilbake rettelsene som er brukt på tidligere identifiserte problemer og skader.

b. Klikk på **Neste**.

Søk etter problemer

Hvis du valgte alternativet **Søk etter skader forårsaket av skadelig programaktivitet**, søker veiviseren etter problemer og mulige skader som skal løses. Når søket er fullført, fortsetter veiviseren automatisk videre til neste trinn.

Velg handlinger for å fikse skader

All skade funnet under det forrige trinnet er gruppert basert på typen fare den utgjør. For hver skadegruppe anbefaler Kaspersky en handlingssekvens for å reparere skaden.

Det finnes tre grupper:

- *Sterkt anbefalte handlinger* eliminerer problemer som representerer en alvorlig sikkerhetstrussel. Vi anbefaler at du reparerer alle skader i denne gruppen.
- *Anbefalte handlinger* er ment å fjerne problemer som utgjør en trussel. Vi anbefaler også at du reparerer skader i denne gruppen.
- *Flere handlinger* reparerer skade på operativsystemet som ikke representerer noen fare nå, men som kan utgjøre en trussel for datasikkerheten i fremtiden.

Utvid listen for den valgte gruppen for å se skade i gruppen.

Hvis du vil at veiviseren skal reparere en bestemt skadetype, merker du av i ruten ved siden av skadebeskrivelsen. Som standard reparerer veiviseren skader som tilhører grupper med anbefalte og sterkt anbefalte handlinger. Hvis du ikke ønsker å reparere en bestemt skadetype, fjerner du avmerkingen i boksen ved siden av skaden.

Vi anbefaler på det sterkeste at du ikke deaktiverer bokser som er aktivert som standard, fordi det vil føre til at datamaskinen blir sårbar for trusler.

Etter at du har definert settet med handlinger som veiviseren skal utføre, klikker du på **Neste**.

Reparere skader

Veiviseren vil utføre handlingene som ble valgt på det forrige trinnet. Det kan ta litt tid å reparere skadene. Når en skade er fikset, fortsetter veiviseren automatisk til neste trinn.

Fullføring av veiviseren

Klikk på **Fullført** for å avslutte veiviseren.

Nødgjenoppretting av operativsystemet

Kaspersky Rescue Disk er beregnet på nødgjenoppretting av operativsystemet. Du kan bruke Kaspersky Rescue Disk til å skanne og desinfisere infiserte datamaskiner som ikke kan desinfiseres, ved å bruke andre metoder (f.eks. med antivirusprogrammer).

Du finner mer informasjon om Kaspersky Rescue Disk på nettstedet til Teknisk støtte.

Slik gjenoppretter du en slettet eller desinfisert fil:

Sikkerhetskopier av slettede eller desinfiserte filer blir plassert i en spesialmappe på datamaskinen som heter *Quarantine*. Sikkerhetskopier av filene lagres i et spesialformat som ikke er farlig for datamaskinen. Du kan gjenopprette en fil som er slettet eller desinfisert fra sikkerhetskopier som er lagret i Quarantine.

Vi anbefaler at du unngår å gjenopprette slettede og desinfiserte filer, ettersom de kan være en trussel for datamaskinen.

Programmet desinfiserer ikke programmer i Windows Store. Hvis skanningsresultatene viser at en slik app er farlig, blir den slettet fra datamaskinen. Når en app i Windows Store blir slettet, oppretter ikke Kaspersky-programmet en sikkerhetskopi av den. Hvis du vil gjenopprette disse objektene, må du bruke gjenopprettingsverktøyene til operativsystemet (se dokumentasjonen til operativsystemet som er installert på datamaskinen, for mer informasjon) eller oppdater programmet fra Windows Store.

Slik gjenoppretter du en slettet eller desinfisert fil:

1. Åpne hovedvinduet.
2. Gå til delen **Sikkerhet**.
3. Klikk på **Karantene** øverst til høyre i vinduet i Kaspersky-programmet.

   Vinduet **Karantene** vil da åpne.
4. I vinduet **Karantene** velger ønsket fil fra listen og klikker på **Gjenopprett**.

Beskytte e-post

Denne delen inneholder informasjon om hvordan du beskytter e-posten din mot virus og andre trusler.

Konfigurere E-post-Antivirus

Kaspersky-programmet tilbyr skanning av e-postmeldinger etter farlige objekter med E-post-Antivirus. E-post-Antivirus starter samtidig med operativsystemet og kjører kontinuerlig i minnet. Det skanner alle e-postmeldinger som sendes og mottas via POP3, SMTP, IMAP og NNTP, men også via krypterte tilkoblinger (SSL) via POP3, SMTP og IMAP.

Som standard skanner E-post-Antivirus både innkommende og utgående e-postmeldinger. Om nødvendig kan du aktivere skanning av kun innkommende meldinger.

Slik konfigurerer du E-post-Antivirus:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Sikkerhetsinnstillinger**.
4. I vinduet **Sikkerhetsinnstillinger** velger du komponenten E-post-Antivirus.

   Dette tar deg til vinduet **Innstillinger for E-post-Antivirus**.
5. Kontroller at bryteren øverst i vinduet, som aktiverer eller deaktiverer E-post-Antivirus, er aktivert.
6. Velg sikkerhetsnivå:

   - **Optimalt**. Hvis dette sikkerhetsnivået er angitt, skanner E-post-Antivirus innkommende og utgående meldinger og kjører en heuristisk analyse med **Middels skanning** som detaljnivå.

- **Lavt**. Hvis du velger dette sikkerhetsnivået, skanner E-post-Antivirus kun innkommende, og skanner ikke vedlagte arkiver.

- **Ekstremt**. Hvis dette sikkerhetsnivået er angitt, skanner E-post-Antivirus innkommende og utgående meldinger og kjører en heuristisk analyse med **Dyp skanning** som detaljnivå.

7. I delen **Handling ved oppdagelse av trussel** velger du handlingen som E-post-Antivirus skal utføre når det oppdages et infisert objekt (for eksempel desinfiser).

Hvis det ikke oppdages trusler i en e-postmelding, eller hvis alle infiserte objekter er desinfisert, blir meldingen tilgjengelig for andre handlinger. Hvis et infisert objekt ikke kan desinfiseres, endrer E-post-Antivirus navnet på objektet eller sletter objektet fra meldingen, og utvider deretter meldingsemnet med en varsling om at meldingen er behandlet av Kaspersky-programmet. Kaspersky-programmet oppretter en sikkerhetskopi av objektet og setter det i Karantene før det slettes.

Når du oppgraderer til en nyere programversjon, blir ikke de brukerkonfigurerte innstillingene for E-post-Antivirus lagret. Den nye programversjonen vil bruke standardinnstillingene for E-post-Antivirus.

Hvis Kaspersky-programmet oppdager passordet for arkivet i meldingsteksten under skanning, brukes passordet til å skanne for skadelig programvare i arkivets innhold. Passordet lagres ikke. Arkivet pakkes ut før skanning. Hvis programmet krasjer under utpakking av arkivet, kan du slette filene som er pakket ut på følgende bane manuelt: %systemroot%\temp. Filene har PR som prefiks.

Blokkere uønsket e-post (spam)

Hvis du mottar store menger uønskede meldinger (spam), anbefaler vi at du aktiverer komponenten Anti-Spam og angir sikkerhetsnivå **Optimalt** for den.

Slik aktiverer du Anti-Spam og stiller inn Optimalt sikkerhetsnivå:

1. Åpne hovedvinduet.

2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.

3. Velg delen **Personverninnstillinger**.

4. Velg komponenten Anti-Spam.

   Vinduet viser innstillingene for Anti-Spam.

5. Aktiver Anti-Spam ved å bruke bryteren.

6. Kontroller i delen **Sikkerhetsnivå** at **Optimalt** sikkerhetsnivå er angitt.

Følgende begrensninger gjelder for Anti-Spam:

- Komponenten Anti-Spam kan kun analysere meldinger som er helt lastet ned fra e-postserveren, uansett hvilken protokoll som brukes.

- Anti-Spam-komponenten sjekker ikke e-post overført ved hjelp av MAPI-protokollen.

Anti-Spam-komponenten deaktiveres når du oppgraderer til en nyere programversjon. Du kan aktivere komponenten manuelt.

I noen versjoner av programmet må du godta vilkårene i erklæringen om databehandling for Anti-Spam for å aktivere komponenten Anti-Spam.

Deltakelse i Kaspersky Security Network.

Kaspersky-programmet bruker skybeskyttelse for å gi mer effektiv beskyttelse av datamaskinen. Skybeskyttelse implementeres ved hjelp av infrastrukturen til Kaspersky Security Network, som bruker data som mottas av brukere verden rundt.

Kaspersky Security Network (KSN) er den skybaserte kunnskapsbasen til Kaspersky, som inneholder informasjon om omdømmet til programmer og nettsteder. Bruk av data fra Kaspersky Security Network gjør det mulig for Kaspersky-programmet å reagere raskere når det oppdages ukjente trusler, øker ytelsen til noen av beskyttelseskomponentene og reduserer faren for falske positive.

Brukere som deltar i Kaspersky Security Network, gjør det mulig for Kaspersky å motta informasjon om nye trusselstyper og -kilder, utvikle løsninger som kan nøytralisere dem og minimere antallet falske positive. Ved å delta i Kaspersky Security Network vil du ha tilgang til omdømmestatistikk for programmer og nettsteder.

Hvis du deltar i Kaspersky Security Network, sender du automatisk informasjon om konfigurasjonen av operativsystemet og oppstarts- og fullføringstidspunktene til prosesser i Kaspersky-programmet til Kaspersky.

Slik aktiverer og deaktiverer du deltagelse i Kaspersky Security Network

Deltakelse i Kaspersky Security Network er valgfritt. Du kan aktivere eller deaktivere Kaspersky Security Network (KSN) når du installerer Kaspersky-programmet, eller når som helst etter at programmet er installert.

Slik aktiverer og deaktiverer du deltagelse i Kaspersky Security Network:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Gå til **Sikkerhetsinnstillinger** → **Kaspersky Security Network**.

   Vinduet **Kaspersky Security Network** åpnes med detaljer om Kaspersky Security Network og deltakelsesinnstillinger for Kaspersky Security Network.
4. Du kan aktivere eller deaktivere deltakelse i Kaspersky Security Network med bryteren øverst i vinduet:

   - Hvis du vil delta i Kaspersky Security Network, setter du bryteren til **På**.

     Et vindu med personvernerklæringen for Kaspersky Security Network åpnes. Hvis du godtar vilkårene i erklæringen, klikker du på **Jeg godtar**.

   - Hvis du ikke ønsker å delta i Kaspersky Security Network, setter du bryteren til **Av**.

I noen versjoner av Kaspersky-programmet viser **Kaspersky Security Network** vinduet **Erklæring for Kaspersky Security Network** i stedet for informasjon om Kaspersky Security Network.

Slik godtar du erklæringen for Kaspersky Security Network:

1. Klikk på **Godta** under **Erklæring for Kaspersky Security Network**.

   Erklæringen for Kaspersky Security Network åpnes. Denne erklæringen gir Kasperskys eksperter tillatelse til raskt å motta informasjon om trusler som oppdages på datamaskinen din, om programmer som kjøres, og signerte programmer som lastes ned, samt operativsysteminformasjon for å forbedre beskyttelsen.

2. Hvis du godtar vilkårene i erklæringen, klikker du på **Godta**.

For å avslå erklæringen for Kaspersky Security Network

klikker du på **Avslå** under **Erklæring for Kaspersky Security Network**.

Slik tester du tilkoblingen til Kaspersky Security Network

Tilkoblingen til Kaspersky Security Network kan være brutt fordi:

- Du deltar ikke i Kaspersky Security Network.
- Datamaskinen ikke er tilkoblet Internett.
- Gjeldende status tillater ikke at du kobler til Kaspersky Security Network. For eksempel kan en forbindelse til KSN være utilgjengelig av følgende årsaker:
  - Programmet er ikke aktivert.
  - Lisens eller abonnement har utløpt.
  - Det har blitt oppdaget problemer med lisensnøkkelen (for eksempel at nøkkelen er lagt til i Avslå-listen).

  Den gjeldende statusen til nøkkelen, vises i My Kaspersky.

Slik sjekker du tilkoblingen til Kaspersky Security Network:

1. Åpne hovedvinduet.
2. Gå til **Sikkerhetsinnstillinger** → **Kaspersky Security Network**.

Vinduet **Kaspersky Security Network** viser statusen for tilkoblingen til Kaspersky Security Network.

Beskyttelse ved hjelp av virtualisering av maskinvare

I denne delen vil du lære hvordan du kan beskytte barna dine ved hjelp av virtualisering av maskinvare.

Om beskyttelse ved bruk av maskinvarevirtualisering

Når Kaspersky-programmet er installert i 64-biters Microsoft Windows 8, Microsoft Windows 8.1 eller Microsoft Windows 10, bruker det hypervisorteknologi for ekstra beskyttelse mot kompleks skadelig programvare som kan fange opp dine personlige data ved hjelp av utklippstavlen eller phishing.

Beskyttelse ved bruk av maskinvarevirtualisering er aktivert som standard. Hvis beskyttelsen er deaktivert manuelt, kan du aktivere den i vinduet for programinnstillinger.

For datamaskiner som kjører 64-biters versjoner av Microsoft Windows 8, Microsoft Windows 8.1 eller Microsoft Windows 10, har beskyttelsen som gis ved bruk av maskinvarevirtualisering i Kaspersky (hypervisor), følgende begrensninger:

- Denne funksjonen er ikke tilgjengelig når en tredjeparts hypervisor kjører, for eksempel hypervisoren som brukes av virtualiseringsprogramvaren VMware™. Når du lukker tredjeparts hypervisorer, vil beskyttelsen mot skjermdumper være tilgjengelig igjen.
- Funksjonen er ikke tilgjengelig hvis CPUen på datamaskinen ikke støtter teknologi for virtualisering av maskinvare. Hvis du vil vite om CPUen støtter virtualisering av maskinvare, kan du se i dokumentasjonen som fulgte med datamaskinen eller søke på nettstedet til CPU-produsenten.
- Funksjonen er ikke tilgjengelig hvis en tredjeparts hypervisor (for eksempel VMware hypervisor) kjører når du starter Beskyttet nettleser.
- Funksjonen er ikke tilgjengelig hvis maskinvarevirtualisering er deaktivert på datamaskinen. For detaljer om hvordan du aktiverer maskinvarevirtualisering på datamaskinen din, kan du se datamaskinens tekniske dokumentasjon eller besøke nettstedet til prosessorprodusenten.
- Funksjonen er ikke tilgjengelig hvis Device Guard er aktivert i operativsystemet Microsoft Windows 10.
- Funksjonen er ikke tilgjengelig hvis Virtualiseringsbasert sikkerhet (VBS) er aktivert i operativsystemet Microsoft Windows 10.

Slik aktiverer du beskyttelse ved bruk av maskinvarevirtualisering

Slik aktiverer du beskyttelse ved bruk av maskinvarevirtualisering:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Gå til **Sikkerhetsinnstillinger** → **Personverninnstillinger** → **Sikkert datainput**.
4. Aktiver avmerkingsboksen **Bruk virtualisering av maskinvare hvis det er tilgjengelig**. Denne avmerkingsboksen vises hvis programmet er installert på en 64-biters versjon av Windows 8, Windows 8.1 eller Windows 10.
5. Velg alternativet **Bruk avanserte funksjoner for virtualisering av maskinvare** hvis du vil at virtualisering av maskinvare skal slås på når operativsystemet starter.

Hvis maskinvarevirtualisering er deaktivert på datamaskinen din, vil beskyttelse ved hjelp av maskinvarevirtualisering deaktiveres.

Beskyttelse ved bruk av Antimalware Scan Interface (AMSI)

Denne delen informerer deg om at tredjepartsprogrammer som Microsoft Office kan sende skripter til Kaspersky-programmet, som skal skannes ved bruk av Antimalware Scan Interface (AMSI), og beskriver hvordan du deaktiverer beskyttelse ved å bruke AMSI i Kaspersky-programmet.

Om beskyttelse ved bruk av Antimalware Scan Interface

Antimalware Scan Interface (AMSI) tillater at tredjepartsprogrammer som støtter AMSI, sender objekter (for eksempel PowerShell-skript) til Kaspersky-programmet for ytterligere skanning og for å motta skanneresultater for disse objektene. Microsoft Office-programmer kan være slike tredjepartsprogrammer. Hvis du vil ha mer informasjon om AMSI-grensesnittet, ser du *Microsoft-dokumentasjonen*.

Antimalware Scan Interface tillater bare oppdagelse av trusler og varsler et tredjepartsprogramm om den oppdagede trusselen. Etter at du har mottatt trusselvarselet, forhindrer tredjepartsprogrammet ondsinnede handlinger (for eksempel avstengning).

Kaspersky-programmet kan avslå en forespørsel fra et tredjepartsprogram hvis for eksempel det aktuelle programmet overstiger det maksimale antallet forespørsler som er tillatt i en periode. I dette tilfellet viser Kaspersky-programmet et varsel om den avslåtte forespørselen. Hvis du mottar en slik varsling, trenger du ikke å gjøre noe som helst.

Beskyttelse ved hjelp av Antimalware Scan Interface er tilgjengelig på Windows 10 Home / Pro / Education / Enterprise og Windows 11 Home / Pro / Enterprise operativsystemer.

Slik aktiverer du beskyttelse ved å bruke Antimalware Scan Interface

Slik aktiverer du beskyttelse ved å bruke Antimalware Scan Interface:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Gå til **Sikkerhetsinnstillinger** → **AMSI-beskyttelse**.
4. I delen **Skriptskanner** merker du av for alternativet **Skann skript som bruker Antimalware Scan Interface (AMSI)**.

Slik utelukker du et skript fra skanning ved å bruke Antimalware Scan Interface

Slik utelukker du et skript fra skanning ved å bruke Antimalware Scan Interface:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Gå til **Sikkerhetsinnstillinger** → **AMSI-beskyttelse**.
4. I delen **Skriptskanner** merker du av for alternativet **Skann skript som bruker Antimalware Scan Interface (AMSI)**.
5. Klikk på koblingen **Behandle unntak** for å åpne vinduet **Unntak**.
6. I **Unntak**-vinduet klikker du på knappen **Legg til**.
   Vinduet **Legg til nytt unntak** åpnes.
7. I feltet **Fil eller mappe** angir du mappen med skriptet.
8. Angi navnet på skriptet i feltet **Objekt**.

   Du kan også legge til flere filer av samme type i unntakene ved å bruke en maske.

9. I delen **Beskyttelseskomponenter** merker du av i boksen ved siden av komponenten Fil-Antivirus.
10. Velg statusen **Aktiv**.

Det angitte objektet skannes ikke av Antimalware Scan Interface.

Ekstern behandling av datamaskinbeskyttelse

Hvis en datamaskin bruker Kaspersky, og er koblet til My Kaspersky, kan du behandle beskyttelsen av denne datamaskinen eksternt.

Logg inn på My Kaspersky-kontoen din og gå til delen **Enheter** for å fjernstyre datamaskinens beskyttelse.

I delen **Enheter** kan du:

- Vise listen over sikkerhetsproblemer på datamaskinen og reparere dem eksternt
- Skanne datamaskinen etter virus og andre trusler
- Oppdatere databaser og programmoduler
- Konfigurere komponentene i Kaspersky

Hvis et datamaskinskann startes fra My Kaspersky, vil Kaspersky behandle objekter som oppdages automatisk, uten at du behøver å gjøre noe. Når et virus eller en annen trussel oppdages, prøver Kaspersky-programmet å desinfisere det uten å starte datamaskinen på nytt. Hvis desinfisering uten omstart av datamaskinen er umulig, viser listen over sikkerhetsproblemer på My Kaspersky en melding om at datamaskinen må startes på nytt for å utføre desinfisering.

Hvis listen over oppdagede objekter på My Kaspersky inneholder mer enn 10 objekter, grupperes de. I slike tilfeller kan de oppdagede objektene kun behandles sammen via My Kaspersky. De kan ikke undersøkes separat. Hvis du vil vise objektene separat, anbefaler vi at du bruker grensesnittet til programmet som er installert på datamaskinen.

Slik går du til ekstern behandling av datamaskinbeskyttelse

Slik går du til ekstern behandling av datamaskinbeskyttelse:

1. Åpne hovedvinduet.
2. Gå til delen **Profil**.
3. I blokken **Logg på My Kaspersky** klikker du på **Logg på**-knappen.
4. Utfør følgende handlinger i vinduet som åpnes:
   - Hvis du har en konto, angir du e-postadressen og passordet og kobler til My Kaspersky.
   - Hvis du ikke har en konto, angir du e-postadresse i tekstboksen og klikker på **Opprett**. En melding med en kobling for oppretting av passord sendes til den angitte e-postadressen.

   Etter en vellykket tilkobling, viser delen **Profil** informasjon om tilkoblingen til kontoen. Du kan nå administrere beskyttelsen av denne datamaskinen eksternt fra My Kaspersky-kontoen din.

Se hjelpedelen for My Kaspersky for mer informasjon om fjernstyring av enhetsbeskyttelse.

Ytelse

Hvis enheten din er tregt eller henger, er du ikke alene om det. Noen ganger nekter programmer å åpne, eller en nettleser slutter å reagere på et avgjørende tidspunkt. Det er flere grunner til at det kan skje. Sørg for enheten kjører stabilt i mange år fremover.

Rask oppstart

Tar det for lang tid å starte datamaskinen? Dette skjer vanligvis når mange programmer startes når operativsystemet starter opp. Vi forteller deg hvilke programmer som bremser datamaskinen når den starter opp, og hjelper deg med å deaktivere autokjør for disse programmene.

Slik gjør du oppstart av datamaskinen raskere:

1. Åpne hovedvinduet.
2. Gå til delen **Ytelse**.
3. Klikk på **Vis programmer**-knappen i delen **Rask oppstart**.

   Vinduet **Gjør oppstart av datamaskinen raskere** åpnes, som viser en liste over programmer som startes ved oppstart.

   Kolonnen **Påvirkning på oppstart** viser informasjon om hvordan hvert program påvirker datamaskinens oppstart. Denne informasjonen er hentet fra operativsystemet og avhenger av hvor mye datamaskinressurser programmet bruker (CPU-belastning og RAM).
4. Velg et program fra listen og sett vekslebryteren **Autokjør** til **Av**.

Programmet vil ikke lenger startes ved oppstart.

PC Speed-Up

Rot bygges opp i et operativsystem over tid og gjør PC-ens tregere. Et stort antall filer som ikke brukes og Windows-registerproblemer bidrar til dette. Kaspersky-programmet vil varsle deg hvis mengden av disse dataene blir for stor, og du vil få en mulighet til å bestemme hvilke data som skal slettes.

Slik rydder du opp i operativsystemet:

1. Åpne hovedvinduet.
2. Gå til delen **Ytelse**.
3. I blokken **Raskere datamaskin** klikker du på **Søk**-knappen (eller **Vis** hvis søket allerede er utført).

   Kaspersky utfører et søk og genererer en rapport med følgende innhold:

   - **Ubrukte systemfiler**. Klikk på knappen **Vis** for å se en detaljert rapport med operativsystemfilene som ikke brukes. Klikk på **Rydd opp** for å slette disse filene.
   - **Problemer med Windows-registeret**. Klikk på knappen **Vis** for å vise en detaljert rapport med problemer i Windows-registeret som du kan slette uten fare for å skade operativsystemet. Klikk på **Reparer** for å reparere oppdagede problemer.

Fjerning av ubrukte filer og reparering av oppdagede problemer vil gjøre PC-en raskere.

Slik deaktiverer du automatisk søk etter måter å gjøre datamaskinen raskere på:

1. Åpne hovedvinduet.
2. Gå til delen **Ytelse**.
3. I blokken **Raskere datamaskin** klikker du på .
4. Deaktiver alternativet **Søk automatisk etter måter å gjøre PC-en raskere på**.

Programoppdatering

Denne delen inneholder informasjon om hvordan du kan bruke Kaspersky-programmet til å oppdatere installerte programmer.

Kun tilgjengelig i Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Om Programoppdatering

Hvis det er lenge siden sist du oppdaterte programmer på datamaskinen, kan disse programmene inneholde sårbarheter. Inntrengere kan utnytte slike sårbarheter til å skade datamaskinen eller dataene dine.

Oppdatering av installerte programmer øker sikkerheten på datamaskinen din. Med Kaspersky-programmet kan du søke etter oppdateringer for installerte programmer og laste ned og installere de siste oppdateringene.

Kaspersky-programmet deler programoppdateringer inn i to typer:

- *Viktig* – oppdateringer som reparerer sårbarhetene til installerte programmer og forbedrer datamaskinens sikkerhet.
- *Anbefalt* – oppdateringer som forbedrer funksjonaliteten og/eller endrer installerte programmer.

Kaspersky-programmet søker regelmessig etter oppdateringer. Når Kaspersky-programmet finner en ny oppdatering for et program installert på datamaskinen din, viser Kaspersky-programmet en popup-melding i systemstatusfeltet. Informasjon om tilgjengeligheten, antallet og typen tilgjengelige oppdateringer vises i varslingssenteret. Du kan vise, laste ned og installere tilgjengelige oppdateringer via varslingssenteret.

Du kan også starte søk etter programoppdateringer manuelt.

Som standard laster Kaspersky-programmet ned og installerer alle oppdateringer for kjente programmer, hvis programmene ikke krever at du aksepterer nye lisensavtaler for sluttbrukere.

I Windows 8 og nyere versjoner, setter Kaspersky-programmet nedlastinger av programoppdateringer på pause når det brukes en tariffbasert internett-tilkobling. Nedlasting av oppdateringer gjenopptas så snart tilkoblingen gjenopprettes. Hvis du har startet oppdateringen manuelt, vil Kaspersky-programmet laste ned oppdateringen selv om du bruker en begrenset tilkobling.

Det kan hende du trenger administratorrettigheter på datamaskinen for å oppdatere enkelte programmer.

Programmer du ikke ønsker å oppdatere, eller som du ikke ønsker å installere enkelte oppdateringer for, plasseres i unntakslisten av Kaspersky-programmet. Du kan vise og redigere unntakslisten.

Før du begynner å søke etter programoppdateringer, kan det hende Kaspersky-programmet krever at du oppdaterer databaser og programmoduler.

Søk etter programoppdateringer

Slik starter du et søk etter programoppdateringer:

1. Åpne hovedvinduet.
2. Gå til delen **Ytelse**.
3. I blokken **Programoppdatering** klikker du på **Søk etter oppdateringer**-knappen.

Dette starter søket etter programoppdateringer.

Slik endrer du innstillinger for Programoppdatering

Slik endrer du innstillinger for Programoppdatering:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Ytelsesinnstillinger**.
4. Klikk på **Programoppdatering**.

   Vinduet **Innstillinger for programoppdatering** vil da åpne.
5. Hvis du ikke vil at Kaspersky-programmet skal laste ned og installere programoppdateringer som ikke krever at du godtar en ny lisensavtale for sluttbrukere automatisk, fjerner du krysset i avmerkingsboksen **Last ned og installer oppdateringer automatisk hvis du ikke må godta nye lisensavtaler**.

   Som standard er dette alternativet aktivert.
6. I delen **Søk etter programoppdateringer** velger du hvilke programoppdateringer som skal lastes ned og installeres av Kaspersky-programmet:

   - Velg **Viktige oppdateringer som forbedrer datamaskinens sikkerhet** hvis du vil at Kaspersky-programmet skal installere kun viktige oppdateringer som reparerer sårbarheter i programvaren og forbedrer datamaskinens sikkerhet.
   - Velg **Alle oppdateringer for kjente programmer** hvis du vil at Kaspersky-programmet skal installere alle programvareoppdateringer.

Slik konfigurerer du Oppdater søkemodus

Slik konfigurerer du søkemodus for oppdateringer for installerte programmer:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Ytelsesinnstillinger**.
4. Klikk på **Programoppdatering**.

   Vinduet **Innstillinger for programoppdatering** vil da åpne.
5. I blokken **Oppdatering** velger du alternativet **Aktiver søk etter programoppdateringer**.
6. Klikk på **Sett opp søkemodus for oppdateringer** for å åpne vinduet **Oppdaterer søkemodus**.
7. I rullegardinlisten **Søk etter oppdateringer** velger du ett av følgende alternativer:

   - **Automatisk**. Hvis du velger dette alternativet, søker Kaspersky-programmet automatisk etter programoppdateringer minst en gang i døgnet i henhold til programmets interne innstillinger.
   - **Hver dag** / **Hver uke** / **Hver måned**. Hvis du velger et av disse alternativene, søker Kaspersky-programmet etter oppdateringer basert på den definerte planen din med minuttnøyaktighet. Når et av disse alternativene er valgt, er listen **Utsett kjøring etter programoppstart for N minutter** tilgjengelig.
8. Velg avkrysningsboksen **Søk etter oppdateringer neste dag hvis datamaskinen er slått av** for å starte et søk når datamaskinen slås på etter at et planlagt søk ikke ble utført. Hvis avkrysningsboksen ikke er valgt, vil programmet bare starte søket etter oppdateringer på det planlagte tidspunktet mens datamaskinen er slått på.
9. For å lagre innstillingene klikker du på **Lagre**.

Vise listen over programoppdateringer

Kaspersky-programmet søker jevnlig etter oppdateringer for programmer installert på datamaskinen din. Informasjon om antall og type oppdateringer for programmer kan vises i varslingssenteret.

Slik viser du listen som genereres når du søker etter programoppdateringer:

1. Åpne hovedvinduet.
2. Klikk på **Detaljer**-knappen øverst i vinduet.

   Vinduet **Varslingssenter** vil da åpne.
3. I delen **Status** klikker du på **Vis** i linjen med melding om tilgjengelige programoppdateringer.

   Dette åpner vinduet **Programoppdatering** med en liste med tilgjengelige programoppdateringer.
4. Klikk på **Oppdater alle** (ikke tilgjengelig i enkelte områder) for å oppdatere alle programmene som vises i listen.
5. Utfør en av følgende handlinger for å velge å oppdatere bestemte programmer:

   - Klikk på **Oppdatering** i linjen som inneholder programmet du ønsker å oppdatere.

Vi anbefaler at du leser lisensavtalen for sluttbrukere før du oppdaterer programmet. Lisensavtalen for sluttbrukere er tilgjengelig i rullegardinlisten **Lisensavtaler**. Som standard er språket i lisensavtalen for sluttbrukere det samme som språket i programmets grensesnitt. Hvis lisensavtalen for sluttbrukere på ikke er tilgjengelig på samme språk som programmets grensesnitt, vises teksten på språket valgt i grensesnittet i Kaspersky-programmet. I alle andre tilfeller vil teksten i lisensavtalen for sluttbrukere være på engelsk, eller det første tilgjengelige språket hvis engelsk tekst ikke er tilgjengelig.

- Klikk på for å åpne menyen og velg **Ikke oppdater dette programmet** hvis du vil at Kaspersky-programmet skal slutte å varsle deg om at det finnes oppdateringer for det valgte programmet.

  Det valgte nettstedet flyttes til unntakslisten. Kaspersky-programmet slutter å vise varslinger om nye oppdateringer som slippes for dette programmet.

- Klikk på for å åpne menyen og velg **Hopp over denne oppdateringen** hvis du vil at Kaspersky-programmet skal slutte å varsle deg om den valgte oppdateringen.

  Den valgte programoppdateringen flyttes til unntakslisten. Kaspersky-programmet viser en varsling om at en ny oppdatering er sluppet for dette programmet.

- Klikk på for å åpne menyen, og velg **Åpne forhandlerens nettsted** hvis du ønsker å laste ned og installere oppdateringen for det valgte programmet manuelt.

  Operativsystemets standard nettleser åpner nettstedet til programvarens leverandør. Du kan vise oppdateringen på nettstedet og laste den ned manuelt.

Dette vinduets grensesnitt, Programoppdatering og visningen av lisensavtalen for sluttbrukere kan variere avhengig av språket i Kaspersky-programmet.

Fjerne en oppdatering eller et program fra unntakslisten

Når du viser listen over programoppdateringer, kan du hoppe over varslinger om individuelle oppdateringer, eller hoppe over varslinger om alle oppdateringer for bestemte programmer. Kaspersky-programmet legger til disse oppdateringene og programmene i unntakslisten.

Slik fjerner du en oppdatering eller et program fra unntakslisten:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Ytelsesinnstillinger**.
4. Klikk på **Programoppdatering**.

   Vinduet **Innstillinger for programoppdatering** vil da åpne.
5. Klikk på **Unntak** for å åpne vinduet **Unntak**.

   Listen **Unntak** inneholder programmer og oppdateringer du har indikert at ikke trenger å oppdateres, i tillegg til enkelte programoppdateringer du ikke installerte.
6. Velg oppdateringen eller programmet i listen, og klikk på **Slett**.

Under neste søk etter oppdateringer vil Kaspersky-programmet varsle deg om tilgjengelige oppdateringer for programmer du har fjernet fra unntakslisten.

Duplikater

Datamaskinen kan lagre filer med identiske filnavn og identisk innhold. Disse dupliserte filene lager rot i minnet, tar opp plass på harddisken og gjør datamaskinen tregere. Du kan finne dupliserte filer og slette ekstra kopier ved å bruke funksjonen Dupliserte filer.

Slik fjerner du dupliserte filer:

1. Åpne hovedvinduet.
2. Gå til delen **Ytelse**.
3. Velg søkeområdet i rullegardinlisten i delen **Duplikater**.
4. Klikk på **Søk**.
5. I søkeresultatvinduet velger du filene og klikker på **Slett**.

Dupliserte filer fjernes fra datamaskinen din, mens de originale dataene bevares.

Store filer

Du prøver å lagre data på datamaskinen, men du finner plutselig ut at harddisken er nesten full. Høres det kjent ut? I dette tilfellet vil du kanskje finne og slette store filer du ikke trenger – vi skal hjelpe deg med dette.

Slik finner du store filer på datamaskinen og fjerner dem:

1. Åpne hovedvinduet.
2. Gå til delen **Ytelse**.
3. I rullegardinlisten **Filer større enn** i delen **Store filer** angir du størrelsen på filene du vil finne, for eksempel **> 1 GB**.
4. Velg en bestemt mappe for søket, eller la standardverdien **Brukermapper** være uendret.
5. Klikk på **Søk**.

   Søket utføres, og vinduet **Store filer** åpnes. Det viser en liste over store filer som ble funnet. Du kan sortere filene etter filtype. Dette gjør du ved å velge en filkategori, for eksempel, **Bilder**.
6. Utfør følgende handlinger:

   - Merk av for **Velg alle** hvis du vil fjerne alle filene, og klikk på **Slett**-knappen.
   - Ellers merker du av i boksene ved siden av bestemte filer og klikker på **Slett**-knappen.

De valgte filene fjernes fra datamaskinen.

Ubrukte programmer

Flere faktorer påvirker datamaskinens ytelse. Antall installerte programmer er en av dem. Jo flere programmer du har installert, desto tregere kjører datamaskinen. Dette forårsakes av at noen programmer, inkludert de som installeres uten at du er klar over det, kan starte automatisk, bruke CPU-ressursene, bruke opp RAM og gjøre unødvendige og noen ganger til og med skadelige handlinger.

Kaspersky-programmet hjelper deg med å finne og fjerne disse programmene.

Slik fjerner du programmer du ikke bruker:

1. Åpne hovedvinduet.
2. Gå til delen **Ytelse**.
3. Klikk på **Søk**-knappen i delen **Ubrukte programmer**.

   Etter at søket er fullført, vil Kaspersky-programmet vise listen over ubrukte programmer. Du kan velge bestemte programmer du vil fjerne i denne listen.
4. Klikk på **Fjern**-knappen ved siden av programmet du vil fjerne.

Programmet fjernes fra datamaskinen din.

Overvåking av harddiskens helse

Denne delen inneholder informasjon om hvordan du kan bruke Kaspersky-programmet til å kontrollere tilstanden til datamaskinens harddisk eller en tilkoblet ekstern harddisk.

Om overvåking av harddiskens tilstand

Kun tilgjengelig i Kaspersky Plus og Kaspersky Premium.

Hvis harddisken din plutselig blir skadet, kan dette føre til tap av data som er lagret på harddisken. Kaspersky-programmet lar deg overvåke tilstanden til harddiskene dine ved bruk av S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology). Denne teknologien er basert på kontinuerlig overvåking av harddiskens sentrale ytelseskarakteristikker. Med Kaspersky-programmet kan du raskt finne ut om harddiskeens tilstand forverres, og kopiere data fra skadede stasjoner til andre medier.

Hvis overvåking av harddiskens tilstand er aktivert, overvåker Kaspersky-programmet harddiskenes tilstand kontinuerlig og varsler deg når tilstanden forverres. Du kan se tilstanden til både interne og eksterne harddisker. Varsler om at harddiskens tilstand forverres, vises i varslingsområdet på oppgavelinjen. Detaljerte rapporter om resultater fra harddiskovervåkingen vises under **Rapporter**.

Hvis harddiskens tilstand forverres og det ikke lenger er sikkert å lagre data på stasjonen, tilbyr Kaspersky-programmet deg å kopiere data fra denne stasjonen til andre medier for å unngå tap av data. Du kan kopiere data fra en skadet harddisk til ethvert godt medium som er tilgjengelig.

Du kan deaktivere overvåking av harddiskens tilstand. Etter at du deaktiverer overvåking av harddiskens tilstand, gir Kaspersky-programmet deg ikke lenger beskjed om endringer i harddiskenes tilstand og gir deg ikke mulighet til å kopiere data fra skadede stasjoner til andre medier.

Slik aktiverer eller deaktiverer du overvåking av harddiskens tilstand

Slik aktiverer eller deaktiverer du overvåking av harddiskens tilstand:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Gå til **Ytelsesinnstillinger** → **PC-ressursforbruk**.
4. Gjør ett av følgende:
   - For å aktivere overvåking av harddiskens tilstand velger du avkrysningsboksen **Utfør skann av harddiskens tilstand**.
   - For å deaktivere overvåking av harddiskens tilstand fjerner du merkingen i boksen **Utfør skann av harddiskens tilstand**.

Slik sjekker du tilstanden til en harddisk

Kaspersky-programmet overvåker kontinuerlig helsen til både interne og eksterne harddisker på datamaskinen din. Overvåkingen jobber i bakgrunnen. Hvis harddiskens tilstand forverres og det ikke lenger er sikkert å lagre data på stasjonen, informerer programmet deg om dette og tilbyr deg å kopiere data til andre medier.

Vinduet **Overvåking av harddiskens helse** viser følgende informasjon om harddisken:

- Stasjonens tilstand.
- Stasjonens temperatur.

Harddisken kan være i en av følgende tilstander:

- *God* – tilstanden til en ny harddisk.
- *Normal* – det er mindre problemer med harddisken.
- *Dårlig* – harddiskens tilstand er kritisk, datatap er mulig.

Harddiskens temperaturområde kan være ett av følgende:

- *Bra* – harddisken er ikke overopphetet.
- *Normal* – temperaturen på harddisken er noe høy.
- *Dårlig* – harddisken er overopphetet.

Figuren **Diskens tilstandshistorikk** viser informasjon om endringer i stasjonens tilstand over den angitte perioden. Maksimal visningsperiode er 1 år.

Kaspersky-programmet viser også følgende statistikk om harddiskene dine:

- *Totalt antall påslåtte timer* – harddiskens totale oppetid i timer.
- *Totalt antall strømsykluser* – antallet ganger harddisken er slått på.

Rapporten **<navn på stasjon> S.M.A.R.T.-attributter** viser informasjon om harddiskens parameterverdier for S.M.A.R.T. sortert etter alvorlighetsgrad. Parametersettet kan variere avhengig av harddiskens produsent og modell.

Slik sjekker du tilstanden til datamaskinens harddisker:

1. Åpne hovedvinduet.
2. Gå til delen **Ytelse**.
3. Under **Ta vare på harddisken og dataene dine**:
   - Hvis du vil se grafen, klikker du på **Historikk**.
   - Hvis du vil se rapporten, klikker du på **Detaljer**.

   Dette tar deg til vinduet der du kan se detaljer om harddiskens tilstand.

Slik kopierer du data fra en skadet harddisk

Hvis tilstanden til en eller flere harddisker på datamaskinen forverres og det ikke lenger er sikkert å lagre data på stasjonene, informerer Kaspersky-programmet deg om dette og gir deg mulighet til å kopiere data fra disse stasjonene til andre medier.

Slik kopierer du dataene fra en skadet harddisk til en harddisk som er i god stand:

1. Gjør ett av følgende:
   - Hvis du mottar et varsel om at harddiskens tilstand forverres, klikker du på **Detaljer** i varslingsvinduet.

     Vinduet **Overvåking av harddiskens helse** åpnes.
   - Klikk på **Kopier data** i vinduet **Overvåking av harddiskens helse**.
2. Klikk på **Start sikkerhetskopiering** i vinduet **Kopierer data** som åpnes.

   Vinduet **Velg lager** vil da åpne.
3. I vinduet **Velg lager** velger du en harddisk som er i god stand for å kopiere data fra den skadde stasjonen.
4. Klikk på **Neste**.

   Vinduet **Velg filer og mapper som skal kopieres** vil da åpne.
5. Gjør ett av følgende:
   - Dra og slipp filer fra Windows Utforsker til det uthevede området i vinduet **Velg filer og mapper som skal kopieres**.
   - Klikk på **velg dem fra listen**-lenken.

     I Utforsker-vinduet som åpnes, kan du velge filer og mapper som skal kopieres til den gode harddisken.

6. Når du har lagt alle filene og mappene du vil kopiere til listen, klikker du på **Neste**.

   Vinduet **Opprette mappe for å kopiere data** vil da åpne.

7. Gjør ett av følgende:

   - Klikk på **Neste** for å opprette en ny mappe på den valgte gode harddisken, og kopier filer og mapper fra den skadede stasjonen til denne.
   - Klikk på **Endre** for å velge en eksisterende mappe på den gode harddisken, og kopier filer og mapper fra den skadede stasjonen til denne.

8. Gjør ett av følgende:

   - Hvis den valgte gode stasjonen har tilstrekkelig diskplass til å kopiere de valgte filene og mappene, klikker du på **Neste** for å starte kopieringen.
   - Hvis den valgte harddisken som er i god stand har utilstrekkelig diskplass til å kopiere de valgte filene og mappene, klikker du på **Tilbake** for å velge en annen harddisk som er i god stand og prøve igjen.

9. Gjør ett av følgende når kopieringen er ferdig:

   - Klikk på **Åpne mappe** for å åpne mappen med filer som ble kopiert fra den skadde harddisken.
   - Klikk på **Fullført** for å lukke vinduet.

Slik kopierer du dataene fra en skadet harddisk til Dropbox' nettbaserte lager.

1. Gjør ett av følgende:

   - Hvis du mottar et varsel om at harddiskens tilstand forverres, klikker du på **Detaljer** i varslingsvinduet.

     Vinduet **Overvåking av harddiskens helse** åpnes.

   - Klikk på **Kopier data** i vinduet **Overvåking av harddiskens helse**.

2. Klikk på **Start sikkerhetskopiering** i vinduet **Kopierer data** som åpnes.

   Vinduet **Velg lager** vil da åpne.

3. I vinduet **Velg lager** velger du Dropbox' nettbaserte lager.

   Du kan også utføre en av følgende handlinger:

   - Klikk på **Aktiver** hvis lageret ikke er aktivt.
   - Hvis du vil deaktivere lageret, klikker du på **Fjern lageret**.

4. Klikk på **Neste**.

   Vinduet **Kopierer data** vil da åpne.

5. Gjør ett av følgende:

   - Dra og slipp filer fra Windows Utforsker til det uthevede området i vinduet **Kopierer data**.
   - Klikk på **velg dem fra listen**-lenken.

     I Utforsker-vinduet som åpnes, kan du velge filer og mapper som skal kopieres til Dropbox' nettbaserte lager.

6. Når du har lagt alle filene og mappene du vil kopiere til listen, klikker du på **Start sikkerhetskopiering**.

   Datakopieringen begynner.

7. Gjør ett av følgende når kopieringen er ferdig:

   - Hvis sikkerhetskopiering av dataene er vellykket, klikker du på **Fullført** for å lukke vinduet.
   - Hvis programmet har varslet deg om at denne sikkerhetskopieringen mislyktes, må du frigjøre plass i det nettbaserte lageret og prøve igjen.

Det er begrensninger for å kopiere data som er lagret i skyen med OneDrive.

Begrensninger for overvåking av harddiskens helse

I noen tilfeller gjør følgende begrensninger at Kaspersky-programmet ikke kan fastslå tilstanden til en harddisk:

- Harddisken støtter ikke S.M.A.R.T-teknologi.
- S.M.A.R.T-funksjonen er slått av på harddisken.
- Kaspersky-programmet støtter ikke:
  - Typen harddisk som er koblet til
  - Typen USB-kontroller på harddisken
- Harddisken er deaktivert.
- Harddisken tilhører en virtuell maskin, for eksempel VMWare. Informasjon om tilstanden til slike harddisker vises ikke, eller vises feil.

Sikkerhetskopiering og gjenoppretting

Dette avsnittet inneholder informasjon om sikkerhetskopiering av data.

Om Sikkerhetskopiering og gjenoppretting

Kun tilgjengelig i Kaspersky Plus og Kaspersky Premium.

Sikkerhetskopiering og gjenoppretting er nødvendig for å beskytte dataene, slik at du ikke mister dem hvis datamaskinen krasjer eller blir stjålet, eller hvis de blir slettet ved et uhell eller skadet av hackere.

Når du vil sikkerhetskopiere data, må du opprette og starte en sikkerhetskopiering. Oppgaven kan startes automatisk i henhold til tidsplanen eller automatisk. Du kan også vise informasjon om fullførte sikkerhetskopieringer.

Vi anbefaler at du lagrer sikkerhetskopier av data på flyttbare stasjoner eller i Nettlagring.

Kaspersky-programmet kan ikke opprette en full kopi av en stasjon mens et Microsoft Windows-operativsystem er aktivt på stasjonen.

I Kaspersky-programmet kan du bruke følgende lagringstyper til å opprette sikkerhetskopier:

- Lokal stasjon
- Flyttbar stasjon (f.eks. en ekstern harddisk)
- Nettverksstasjon
- Nettlagring.

Opprette oppgaver basert på brukerens tilgangsrettigheter

Sikkerhetskopieringsoppgaver opprettes basert på brukerens tilgangsrettigheter til filer på den lokale datamaskinen.

Hvis du ikke har lokale administratorrettigheter på datamaskinen, har du kun tilgang til oppgaver du har opprettet selv. Hvis du har lokale administratorrettigheter på datamaskinen, kan du se alle sikkerhetskopieringsoppgaver men ikke endre oppgaver opprettet av andre brukere.

Sikkerhetskopieringsoppgaver som ble opprettet tidligere uten å ta hensyn til brukerrettigheter er tilgjengelige for alle brukere av datamaskinen. Hvis en slik oppgave endres, vil den imidlertidig kjøre basert på rettighetene til brukeren som endret oppgaven.

Gjenopprette oppgaver basert på brukerens tilgangsrettigheter

Hvis du ikke har lokale administratorrettigheter på datamaskinen, kan du kun gjenopprette data fra sikkerhetskopieringsoppgaver du har opprettet selv, og kun til mappene du har tilgangsrett til. Hvis du har lokale administratorrettigheter på datamaskinen, kan du gjenopprette data fra alle sikkerhetskopieringsoppgaver til hvilken som helst mappe.

Den totale størrelsen til kopierte filer i en mappe som kan overgå størrelsen til mappen hvis den inneholder lenker til andre filer (for eksempel vil mappene Min Musikk, Mine bilder og Mine videoer også bli kopiert hvis du kopierer til mappen Dokumenter og den inneholder lenker til disse mappene).

Om sikkerhetskopiering og gjenoppretting i OneDrive

Når du sikkerhetskopierer filer til en OneDrive-mappe på datamaskinen, fungerer Kaspersky-programmet annerledes, avhengig av om skyfilen er lastet ned til OneDrive-mappen:

- Hvis filen er i skyen og i OneDrive-mappen på datamaskinen, oppretter Kaspersky-programmet en sikkerhetskopi av denne filen.
- Hvis filen ikke er i skyen, men den er til stede i OneDrive-mappen på datamaskinen, oppretter Kaspersky en sikkerhetskopi av denne filen.
- Hvis filen vises i OneDrive-mappen, men den bare er lagret i skyen og ikke på datamaskinen, oppretter Kaspersky-programmet en sikkerhetskopi av denne filen.

Slik oppretter du en sikkerhetskopiering

Slik oppretter du en sikkerhetskopiering:

1. Åpne hovedvinduet.
2. Velg delen **Ytelse**.
3. I blokken **Sikkerhetskopiering og gjenoppretting** klikker du på **Velg filer**-knappen.

   Veiviseren for oppretting av sikkerhetskopieringsoppgave startes.

   Veiviseren består av en rekke skjermbilder (trinn) som du kan navigere i med knappene **Tilbake** og **Neste**. Klikk på **Fullført**-knappen for å lukke veiviseren når den er fullført. Du kan når som helst stoppe veiviseren ved å klikke på **Avbryt**.

   La oss gå grundigere gjennom trinnene i veiviseren.

Trinn 1. Velg filer

På dette trinnet i veiviseren velger du typen filer eller angir mappene du vil sikkerhetskopiere:

- Velg en av de forhåndsdefinerte filtypene (filer fra mappene Mine dokumenter og skrivebordet, videoer, bilder, musikkfiler) hvis du ønsker en rask konfigurasjon. Hvis du bekrefte dette alternativet, tar veiviseren deg direkte til trinn 4 Velg sikkerhetskopilager.

  > Kaspersky-programmet oppretter ikke sikkerhetskopier av filer i mappene Skrivebord og Mine dokumenter, dersom disse mappene er lagret på en nettverksstasjon.

- Merk av for **Opprett sikkerhetskopier av filer fra angitte mapper** hvis du vil angi filer og mapper som skal sikkerhetskopieres, manuelt.

Trinn 2. Velg mapper for sikkerhetskopiering

Hvis du har aktivert alternativet **Opprett sikkerhetskopier av filer fra angitte mapper** på forrige trinn i veiviseren, klikker du på **Legg til mappe**. Vinduet **Velg mappe for sikkerhetskopiering** åpnes, der du kan velge en mappe eller dra mappen inn i programvinduet.

Merk av for alternativet **Begrens sikkerhetskopiering etter filtyper** hvis du vil angi kategorier med filer som skal sikkerhetskopieres i de valgte mappene.

Trinn 3. Velg filtyper som skal sikkerhetskopieres

Hvis du har aktivert alternativet **Begrens sikkerhetskopiering etter filtyper** på forrige trinn i veiviseren, aktiverer du avmerkingsboksene ved siden av filtypene du vil sikkerhetskopiere, i det neste vinduet.

Trinn 4. Velg sikkerhetskopilager

På dette trinnet velger du et sikkerhetskopilager:

- **Nettbasert lager**. Velg dette alternativet hvis du vil lagre sikkerhetskopier i det nettbaserte Dropbox-lageret. Nettbasert lagring må aktiveres før det kan brukes. Når du sikkerhetskopierer data til Nettlagring, oppretter ikke Kaspersky-programmet sikkerhetskopier av datatyper som er underlagt begrensninger i bruksreglene til Dropbox.
- **Lokal stasjon**. Hvis du vil lagre sikkerhetskopier på en lokal stasjon, velger du den aktuelle lokale stasjonen i listen.
- **Nettverksstasjon**. Hvis du vil lagre sikkerhetskopier på en nettverksstasjon, velger du den aktuelle nettverksstasjonen i listen.
- **Flyttbar stasjon**. Hvis du vil lagre sikkerhetskopier på en flyttbar stasjon, velger du den aktuelle stasjonen i listen.

Av hensyn til datasikkerhet, anbefaler vi at du bruker Lagring på nett eller oppretter sikkerhetskopilagre på flyttbare stasjoner.

Slik legger du til nettverkslager

Slik legger du til et nettverkslager:

1. Klikk på **Legg til nettverkslager** for å åpne vinduet **Legg til nettverkslager** og velge nettverkslageret.
2. Angi dataene som kreves for å koble til nettverkslageret.
3. Klikk på **OK**.

Slik legger du til en flyttbar stasjon som lager

Slik legger du til en flyttbar stasjon som sikkerhetskopilager:

1. Klikk på koblingen **Koble til eksisterende lager** for å åpne vinduet **Koble til lager**.
2. Velg delen **Flyttbar stasjon**.
3. Klikk på **Bla gjennom** og angi den flyttbare stasjonen du vil lagre sikkerhetskopier på, i vinduet som åpnes.

Merk av for alternativet **Bruk avanserte lagringsinnstillinger** for å konfigurere innstillinger for fillagring, for eksempel antall sikkerhetskopiversjoner som skal lagres, og lagringstiden for sikkerhetskopier.

Trinn 5. Opprette en sikkerhetskopieringsplan

På dette trinnet i veiviseren gjør du ett av følgende:

- Angi en sikkerhetskopieringsplan hvis du vil at sikkerhetskopieringer skal startes automatisk.

  a. I rullegardinlisten **Kjør sikkerhetskopiering** velger du en tidsintervall for kjøring av oppgaven (for eksempel **hver dag**) og angir klokkeslettet oppgaven skal kjøres i feltet **Kl**.

  b. I delen **Konto** angir du brukernavn og passord for Windows-kontoen din på denne datamaskinen. Dataene for Windows-kontoen din kreves for å få tilgang til filer under sikkerhetskopiering.

  c. Velg alternativet **Kjør planlagt sikkerhetskopiering ved oppstart av datamaskinen hvis funksjonen var slått av på angitt tidspunkt** hvis du vil at det skal kjøres en sikkerhetskopi så snart som mulig etter at datamaskinen er slått på. La oss for eksempel si at sikkerhetskopieringen skal kjøres hver helg. Hvis datamaskinen var slått av over helgen, kjøres sikkerhetskopieringen straks datamaskinen slås på, selv om det er på en ukedag. Hvis alternativet er deaktivert, kjøres sikkerhetskopieringen i henhold til tidsplanen, sikkerhetskopieringer som ikke er fullført, vil ikke blir kjørt på nytt.

- I listen **Kjør sikkerhetskopiering** velger du alternativet **på forespørsel** hvis du vil starte oppgaven manuelt.

Vær oppmerksom på følgende når du jobber med sikkerhetskopieringsoppgaver:

- Hvis du oppretter en planlagt sikkerhetskopieringsoppgave, må du angi dataene for kontoen din på denne datamaskinen.

- Hvis du oppretter en sikkerhetskopieringsoppgave som skal kjøres ved behov, trenger du ikke å angi dataene for kontoen din på denne datamaskinen.

- Hvis du endrer en oppgave ved behov til en planlagt sikkerhetskopieringsoppgave, må du angi dataene for kontoen din på denne datamaskinen.

Trinn 6. Angi et passord for å beskytte sikkerhetskopier

Velg **Aktiver passordbeskyttelse**, og fyll ut feltene **Passord for tilgang til sikkerhetskopier** og **Bekreft passord** for å beskytte tilgangen til sikkerhetskopier med et passord.

Passordet er nødvendig for å beskytte lagring av sikkerhetskopi mot uautorisert tilgang.

Programmet vil be deg om å skrive inn et passord i følgende tilfeller:

- Når du først oppretter en sikkerhetskopilagring på en lokal eller flyttbar stasjon (som en flash-enhet). Når du oppretter etterfølgende sikkerhetskopioppgaver til en lokal stasjon eller denne flyttbare stasjonen, vil programmet ikke lenger be deg om å skrive inn et passord. Passordet du skrev inn tidligere vil bli brukt.

  Hvis du kopierer den lokale sikkerhetskopilagringen til en flyttbar stasjon og kobler denne flyttbare stasjonen til en annen datamaskin, vil programmet be deg om å skrive inn et passord for å kopiere eller gjenopprette data fra denne stasjonen.

- Når du kobler til en flyttbar stasjon til datamaskinen. Programmet sjekker den flyttbare stasjonen og ber deg om å skrive inn et passord hvis den oppdager en sikkerhetskopi på denne flyttbare stasjonen.

Trinn 7. Innstillinger for lagring av filversjoner

Dette trinnet er tilgjengelig hvis alternativet **Bruk avanserte lagringsinnstillinger** ble aktivert på trinn 4 «Velg sikkerhetskopilager».

Spesifiser fillagringsinnstillingene:

- Merk av for alternativet **Begrens antall versjoner av sikkerhetskopier**, og angi antall sikkerhetskopier av én fil som skal lagres, i listen **Versjoner av sikkerhetskopier som skal lagres**.
- Merk av for alternativet **Begrens lagringsperioden for versjoner av sikkerhetskopier**, og angi antall dager for lagring av hver sikkerhetskopiversjon i feltet **Behold gamle versjoner av sikkerhetskopier i**.

Trinn 8. Skrive inn et navn for sikkerhetskopieringen

Gjør følgende på dette trinnet:

- Skriv inn navnet på sikkerhetskopieringen
- Velg **Kjør sikkerhetskopiering når oppsettet er ferdig** for å starte sikkerhetskopieringsprosessen automatisk når veiviseren er fullført

Trinn 9. Fullføring av veiviseren

Dette vinduet vises fremdriften for konfigurering av sikkerhetskopilageret. Konfigurasjonsprosessen kan ta litt tid.

Når konfigurasjonen er ferdig, klikker du på **Fullført**.

En sikkerhetskopiering opprettes. Oppgaven du har opprettet, vises i vinduet **Sikkerhetskopiering og gjenoppretting**.

Slik starter du en sikkerhetskopiering

Slik starter du en sikkerhetskopiering:

1. Åpne hovedvinduet.
2. Velg delen **Ytelse**.
3. I blokken **Sikkerhetskopiering og gjenoppretting** klikker du på **Vis sikkerhetskopier**-knappen.
4. I vinduet **Sikkerhetskopiering og gjenoppretting** som åpnes, klikker du på **Kjør**.

   Sikkerhetskopieringen startes.

Gjenopprette data fra en sikkerhetskopi

Slik gjenoppretter du data fra en sikkerhetskopi:

1. Åpne hovedvinduet.
2. Velg delen **Ytelse**.
3. I blokken **Sikkerhetskopiering og gjenoppretting** klikker du på **Vis sikkerhetskopier**-knappen.

   Vinduet **Sikkerhetskopiering og gjenoppretting** vil da åpne.

   - Klikk på **Gjenopprett filer** ved siden av den aktuelle sikkerhetskopieringen.
   - Klikk på **Behandle lagre** for å åpne et vindu, og klikk på **Gjenopprett filer** ved siden av det aktuelle lageret.
4. Hvis et passord ble angitt da sikkerhetskopien ble opprettet, oppgir du dette passordet i vinduet **Skriv inn passord for å åpne lageret**.
5. Velg dato og klokkeslett for opprettelse av sikkerhetskopien i rullegardinlisten **Dato/klokkeslett for sikkerhetskopiering**.
6. Gjør ett av følgende:

   - Hvis du vil gjenopprette alle data, merker du av for alternativet **Alle data**.
   - Hvis du kun vil gjenopprette enkelte mapper, merker du av i rutene ved siden av de aktuelle mappene.
   - Hvis du kun vil gjenopprette bestemte filer, merker du av i rutene ved siden av de aktuelle filene i kolonnen **Navn**.
7. Hvis du kun vil gjenopprette bestemte typer filer, velger du disse filtypene i rullegardinlisten **Filtype**.
8. Klikk på **Gjenopprett valgte filer**.

   Vinduet **Gjenopprett filer fra sikkerhetskopier** vil da åpne.
9. Velg ett av disse alternativene:

   - **Opprinnelig mappe**. Hvis dette alternativet er valgt, gjenopprettes data til den opprinnelige mappen.
   - **Angitt mappe**. Hvis dette alternativet er valgt, gjenopprettes data i den angitte mappen. Klikk på **Bla gjennom** for å velge mappen du vil gjenopprette data i.
10. Fra rullegardinlisten **Hvis filnavn ikke samsvarer** velger du handlingen som skal utføres når navnet på filen som gjenopprettes, samsvarer med navnet på en fil som allerede finnes i målmappen:

    - **spør** – hvis det oppdages samsvarende filnavn, blir du bedt om å velge ett av disse alternativene: Erstatte filen med sikkerhetskopien, lagre begge filene eller ikke gjenopprette filen.
    - **erstatt filen med sikkerhetskopien** – Kaspersky-programmet sletter den eksisterende filen og erstatter den med den gjenopprettede filen fra sikkerhetskopien.
    - **lagre begge filene** – Kaspersky-programmet beholder den eksisterende filen og lagrer den gjenopprettede filen fra sikkerhetskopien med et nytt navn i samme mappe.

- **ikke gjenopprett denne filen** – Kaspersky-programmet beholder den eksisterende filen og gjenoppretter ikke filen med samme navn fra sikkerhetskopien.

11. Klikk på **Gjenopprett**.

    Filene som er valgt for gjenoppretting, gjenopprettes fra sikkerhetskopien og lagres i den angitte mappen.

Gjenopprette data fra FTP-lager

Kaspersky-programmet støtter ikke sikkerhetskopiering og gjenoppretting over FTP. Følg instruksjonene nedenfor for å gjenopprette sikkerhetskopier som er opprettet i andre Kaspersky-programmer fra FTP-lageret.

Slik gjenoppretter du sikkerhetskopier fra FTP-lageret:

1. Åpne hovedvinduet.
2. Velg delen **Ytelse**.
3. I blokken **Sikkerhetskopiering og gjenoppretting** klikker du på **Vis sikkerhetskopier**-knappen.

   Vinduet **Sikkerhetskopiering og gjenoppretting** vil da åpne.
4. Klikk på **Behandle lagre** for å åpne vinduet **Lagre**.
5. Åpne FTP-lagringsmappen i Windows Utforsker.
6. Kopier dataene (inkludert filen `storage.xml`) til en lokal disk (for eksempel C: \<mappenavn>).
7. I vinduet **Lagre** ved siden av FTP-lageret klikker du på **Slett lager**.
8. Klikk på **Slett** i vinduet for bekreftelse av slettingen.

   Lageret er nå slettet.
9. I vinduet **Lagre** klikker du på **Koble til eksisterende lager**.
10. I vinduet **Koble til lager** velger du delen **Lokal stasjon** og bruker **Bla gjennom** for å spesifisere banen til mappen som inneholder sikkerhetskopiene du kopierte til den lokale stasjonen fra FTP-lageret.
11. I vinduet **Lagre**, ved siden av det tilkoblede lageret klikker du på **Gjenopprett filer**.
12. Følg standard fremgangsmåte for gjenoppretting.

Gjenopprette data fra en sikkerhetskopi med Kaspersky Restore Utility

Kaspersky Restore Utility lar deg administrere lagret data fra en sikkerhetskopi på en datamaskin der et Kaspersky-program er ødelagt eller har blitt fjernet. Etter at du har installert verktøyet, vil det som standard være plassert i mappen Kaspersky Restore Utility, som ligger i programmets installasjonsmappe. Hvis du vil bruke verktøyet på en datamaskin der Kaspersky-programmet ikke er installert, eller er skadet, må verktøyet kopieres til en flyttbar stasjon.

Du må ha lokale administratorrettigheter for å starte Kaspersky Restore Utility.

Slik starter du Restore Utility

Slik starter du Restore Utility:

1. Åpne den flyttbare stasjonen du har kopiert verktøyet til.
2. Kjør filen kasperskylab.pure.restoretool i mappen Kaspersky Restore Utility.

   Hovedvinduet til Restore Utility åpnes. Vinduet viser standardlageret som er konfigurert i programmet. Du kan spesifisere banen til et annet lager.

Slik åpner du et laget med Restore Utility

Slik åpner du et lager med Restore Utility:

1. Start Restore Utility.

   Verktøyet oppdager automatisk banen til sikkerhetskopilageret, hvis den er opprettet på den lokale C:-stasjonen.
2. Hvis sikkerhetskopilageret er plassert på en annen stasjon, klikker du på knappen **Angi lager** i hovedvinduet i Restore Utility.
3. I vinduet som åpnes, klikker du på knappen **Bla gjennom** og angir banen til sikkerhetskopilageret.
4. Klikk på **Velg lager**.

Slik gjenoppretter du data fra en sikkerhetskopi

Slik gjenoppretter du data fra en sikkerhetskopi:

1. Start Restore Utility.
2. Følg denne fremgangsmåten i hovedvinduet til Restore Utility:
   a. I rullegardinlisten **Sikkerhetskopiering** velger du oppgaven som opprettet sikkerhetskopiene du trenger.
   b. Velg datoen og klokkeslettet da de aktuelle sikkerhetskopiene ble opprettet, i rullegardinlisten **Dato/klokkeslett for sikkerhetskopiering**.
3. Velg filene du vil gjenopprette. Det gjør du ved å merke av i boksene ved siden av de aktuelle mappene i listen.

   Bruk knappen ved siden av **Søk**-feltet til å veksle mellom et mappetre og en liste med filer.
4. Klikk på **Gjenopprett valgte filer**.

   Vinduet **Velg hvor du vil plassere gjenopprettede filer** vil da åpne.
5. Velg plasseringen der du vil lagre gjenopprettede filer, i vinduet som åpnes.
   - **Opprinnelig mappe**. Velg dette alternativet for å gjenopprette data til den originale mappen.
   - **Angitt mappe**. Velg dette alternativet for å velge mappen du vil gjenopprette data i. Klikk på **Bla gjennom** for å velge mappen der dataene skal gjenopprettes.
6. I rullegardinlisten **Hvis filnavn ikke samsvarer** kan du velge en handling som skal utføres av programmet når målmappen for filen som blir gjenopprettet, allerede inneholder en fil med samme navn:
   - **spør** – hvis det oppdages samsvarende filnavn, blir du bedt om å velge ett av disse alternativene: Erstatte filen med sikkerhetskopien, lagre begge filene eller ikke gjenopprette filen.
   - **erstatt filen med sikkerhetskopien** – Kaspersky-programmet sletter den eksisterende filen og erstatter den med den gjenopprettede filen fra sikkerhetskopien.
   - **lagre begge filene** – Kaspersky-programmet beholder den eksisterende filen og lagrer den gjenopprettede filen fra sikkerhetskopien med et nytt navn i samme mappe.
   - **ikke gjenopprett denne filen** – Kaspersky-programmet beholder den eksisterende filen og gjenoppretter ikke filen med samme navn fra sikkerhetskopien.
7. Klikk på **Gjenopprett**.

   Vinduet **Gjenopprett filer** vil da åpne. Vinduet viser fremgangen til gjenopprettingen av filer fra sikkerhetskopier. Du kan når som helst stoppe gjenopprettingsprosessen ved å klikke på **Stopp**-knappen.

   De nødvendige sikkerhetskopiene av de valgte filene, gjenopprettes.

Om Nettlagring

Med Kaspersky-programmet kan du lagre sikkerhetskopier av data i Nettlagring på en ekstern server via Dropbox-tjenesten.

Slik bruker du Nettlagring:

- Kontroller at datamaskinen er tilkoblet Internett.
- Opprett en konto på nettstedet til tjenesteleverandøren for det nettbaserte lageret.
- Aktivere Nettlagring.

Du kan bruke samme Dropbox-konto til å sikkerhetskopiere data fra forskjellige enheter som har Kaspersky installert, til ett lager for nettlagring.

Størrelsen på det nettbaserte lageret bestemmes av tjenesteleverandøren, nettjenesten Dropbox. Se nettstedet til Dropbox for å finne ut mer om bruksvilkårene til webtjenesten.

Når du kopierer filer til Dropbox, skiller ikke Kaspersky-programmet mellom store og små bokstaver i navnet på en fil og/eller navnet til en bane til filen. Når du prøver å lage sikkerhetskopier av filer med navn og/eller baner der den eneste forskjellen er store og små bokstaver, oppretter Kaspersky-programmet bare én sikkerhetskopi fordi det oppstår en konflikt i Dropbox.

Slik aktiverer du Nettlagring

Slik aktiverer du Nettlagring:

1. Åpne hovedvinduet.
2. Velg delen **Ytelse**.
3. I blokken **Sikkerhetskopiering og gjenoppretting** klikker du på **Velg filer**-knappen.

   Veiviseren for oppretting av sikkerhetskopieringsoppgave startes.
4. I vinduet for valg av datatype angir du datakategorien eller velger filene du vil sikkerhetskopiere manuelt.
5. I vinduet for valg av lagring velger du alternativet **Nettbasert lager** og klikker på **Aktiver**.

   Internett-tilkobling er nødvendig for å bruke Nettlagring.

   En dialog for innlogging på Dropbox-konto vises.
6. Utfør følgende handlinger i vinduet som åpnes:
   - Fullfør registreringen hvis du ikke er en registrert bruker av Dropbox.
   - Hvis du er registrert Dropbox-bruker, logger du deg inn på Dropbox-kontoen din.
7. Du fullfører aktiveringen av Nettlagring ved å bekrefte at Kaspersky-programmet kan bruke Dropbox-kontoen til å sikkerhetskopiere og gjenopprette data. Kaspersky-programmet plasserer sikkerhetskopier av lagrede data i en separat mappe som er opprettet i lagringsmappen for programmer på Dropbox.

   Når aktiveringen av Nettlagring er fullført, åpnes vinduet for valg av lager. Det inneholder et utvalg av nettbaserte lager du kan velge mellom. Programmet viser både brukt og tilgjengelig lagringsplass for det aktiverte lageret for Nettlagring.

Når du kopierer filer til Dropbox, skiller ikke Kaspersky-programmet mellom store og små bokstaver i navnet på en fil og/eller navnet til en bane til filen. Når du prøver å lage sikkerhetskopier av filer med navn og/eller baner der den eneste forskjellen er store og små bokstaver, oppretter Kaspersky-programmet bare én sikkerhetskopi fordi det oppstår en konflikt i Dropbox.

Gjeldende aktivitet

Hvis du har lagt merke til at datamaskinen fryser eller er tregere, kan du åpne vinduet **Programaktivitet**. Dette vinduet viser en liste over programmer som kjører og aktive prosesser, og avslutter ett eller flere programmer som bruker for mye av datamaskinens ressurser.

Slik ser du gjeldende aktivitet og/eller avslutter et program:

1. Åpne hovedvinduet.
2. Gå til delen **Ytelse**.
3. I blokken **Gjeldende aktivitet** klikker du på **Vis aktivitet**-knappen.

   Dette åpner vinduet **Programaktivitet**, der fanen **Kjører** er åpen.
4. Fra listen med programmer velger du det som bruker mest prosessorressurser (i **CPU**-kolonne-) og/eller RAM (i **Minne**-kolonnen), og klikker på **Avslutt prosess**-knappen.

Programmet vil da avsluttes.

Ikke forstyrr-modus

I ikke forstyrr-modus viser ikke Kaspersky-programmet popup-varslinger om sikkerhetshendelser på datamaskinen mens du jobber, studerer, er i en videosamtale eller ser på en film. Ikke forstyrr-modus aktiveres og deaktiveres automatisk. Du trenger ikke å endre programinnstillingene.

Etter at du har avsluttet Ikke forstyrr-modus, bruker programmet oppgavelinjens varslingsområde til å vise en melding om enhver hendelse som skjedde mens du var opptatt. Hvis det var flere hendelser, klikker du på **Vis**-knappen for å gå til **Varslingssenter** og se alle hendelsene.

Du kan også se alle hendelser som har skjedd i løpet av de siste tre dagene i **Varslingssenter** på fanen **Status** i delen **Varslinger**.

Se hjelpedelen Om varsler for mer informasjon om visning av varsler.

Spillmodus

Når Kaspersky-programmet kjører i fullskjermsmodus med andre programmer (spesielt for dataspill), kan følgende problemer oppstå:

- Program- eller spillytelsen blir redusert på grunn av mangel på systemressurser

- Vinduet med varslinger i Kaspersky-programmet distraherer brukeren fra spillet

Hvis du ikke vil endre innstillingene i Kaspersky-programmet manuelt hver gang du bytter til fullskjermsmodus, kan du bruke spillmodus. Hvis spillmodus brukes og du spiller eller jobber med programmer i fullskjermmodus, kjører Kaspersky-programmet ikke skanne- og oppdateringsoppgaver og viser ikke varsler.

Slik aktiverer du spillmodus:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Gå til **Ytelsesinnstillinger** → **PC-ressursforbruk**.
4. Aktiver avmerkingsboksen **Spillmodus**.

Du kan også krysse av for **Ikke forstyrr-modus**. I denne modusen vil du ikke få se varsler hvis du aktiv arbeider i enkelte programmer, og skanne- og oppdateringsoppgaver startes ikke.

Batterisparer

Når Batterisparer-modus er aktivert, utsetter Kaspersky-programmet planlagte skanne- og oppdateringsoppgaver. Du kan starte skanning og oppdatere oppgaver manuelt ved behov.

Du kan også aktivere eller deaktivere Batterisparer-modus i vinduet **PC-ressursforbruk** ved å velge eller fjerne merkingen for **Batterisparer**.

Optimalisering av belastningen på operativsystemet

Når du kjører en dataskanning ved å bruke Kaspersky-programmet, kan den bruke betydelige systemressurser. Du kan optimalisere belastningen på systemet ved å konfigurere Kaspersky-programmet til å kjøre skanneoppgaver (systemminne, systempartisjon og oppstartsobjekter) og oppdatere databaser når datamaskinen er låst eller skjermspareren er aktivert. Med denne tilleggsinnstillingen kan du forbedre sikkerheten til datamaskinen uten at det påvirker ytelsen når du bruker den.

Hvis datamaskinen kjører på batteri, kjører ikke Kaspersky-programmet oppgaver når datamaskinen er inaktiv, for å forlenge batterilevetiden.

Slik optimaliserer du belastningen på operativsystemet:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Gå til **Ytelsesinnstillinger** → **PC-ressursforbruk**.
4. Aktiver avmerkingsboksen **Utsett skanneoppgaver når det er høy belastning på prosessoren og disksystemene**.

Personvern

Nåtidens massive datainnbrudd og markedsførere som sporer alt du gjør på nettet – listen over digitale irritasjonsmomenter fortsetter og fortsetter. Beskyttelse av personvern er avgjørende. Lær hvordan Kaspersky-programmet beskytter personvernet ditt på nett, slik at du kan administrere og kontrollere det digitale fotavtrykket ditt.

Kaspersky VPN

Kun tilgjengelig i Kaspersky Plus og Kaspersky Premium.

VPN-tilkoblingen opprettes med Kaspersky VPN Secure Connection, som tilbys som en del av Kaspersky Plus-abonnementet. Du kan starte Kaspersky VPN Secure Connection fra **Start**-menyen (i Microsoft Windows 7 eller tidligere operativsystemer), fra startskjermen (i Microsoft Windows 8 eller nyere operativsystemer) eller fra vinduet i Kaspersky-programmet.

Slik starter du Kaspersky VPN Secure Connection fra vinduet i Kaspersky-programmet:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. I blokken **Kaspersky VPN** klikker du på **Åpne**-knappen.

   Dette åpner hovedvinduet for Kaspersky VPN Secure Connection.

Du finner mer informasjon om operasjonen til Kaspersky VPN Secure Connection i programmets hjelpefil.

Datalekkasjekontroll

Denne delen forklarer hvordan du skal sjekke om brukerkontodataene dine er offentlig tilgjengelig.

Om Datalekkasjekontroll

Med Kaspersky Basic og Kaspersky Standard vil Datalekkasjekontroll bare la deg sjekke My Kaspersky-kontoen manuelt. Automatiske kontroller for My Kaspersky-kontoen din og andre kontoer er kun tilgjengelig for Kaspersky Plus- og Kaspersky Premium.

De fleste brukere lager kontoer på ulike nettsteder for arbeid, shopping og kommunikasjon. Det er alltid en risiko for at angripere kan hacke siden og få tilgang til brukerdata. Hvis du bruker samme e-postadresse og passord for forskjellige nettsteder, er det mer sannsynlig at dataene dine blir lekket.

Med Kaspersky-programmet kan du sjekke brukerkontoene dine for potensielle lekkasjer. Hvis sjekken avslører at dataene dine kan være tilgjengelig for offentligheten, vil programmet varsle deg om dette og vise en liste over nettsteder hvor det kan ha oppstått en datalekkasje, datoen for mulig lekkasje og kategorien data som kan være offentlig tilgjengelig.

Kaspersky-programmet sjekker også kontoene dine for datalekkasjer til Darknet. Hvis det oppdages en lekkasje, advarer programmet deg om det.

Når du kontrollerer brukerkontoer, henter ikke Kaspersky data i rentekstform og bruker dem bare for den angitte kontrollen uten å lagre dem. Når en lekkasje oppdages, får ikke Kaspersky-programmet tilgang til selve brukerdataene, men gir bare informasjon om kategorier av data som kan være offentlig tilgjengelig.

Kaspersky-programmet kan varsle deg om en eventuell lekkasje av følgende datakategorier:

- **Personlige data**: for eksempel passdata, biometriske data, data om alder.
- **Bankdata**: for eksempel antall kredittkort og bankkontoer, informasjon om midler tilgjengelig på kredittkort og bankkontoer.
- **Aktivitetshistorikk**: for eksempel autentiseringstokener, passordhistorikk.

Som standard forsøker Kaspersky-programmet å sjekke brukerkontoene dine når du autoriseres på et bestemt nettsted. Under autorisasjonen krypteres e-postadressen din som brukes til å logge på nettstedet og videresendes til KSN-cloud. Hvis sjekken avslører at dataene dine kan være offentlig tilgjengelig, vil du motta en melding om dette. Du kan deaktivere Datalekkasjekontroll.

Du kan legge til opptil 50 kontoer som skal sjekkes automatisk. Lister over kontoer i Kaspersky-programmet synkroniseres ikke mellom enheter. Kontoene som er lagt til sjekkes én gang hver dag.

Det kan hende at legge til kontoer i listen for automatisk sjekking ikke er tilgjengelig i området du bor i.

Kaspersky-programmet sjekker med jevne mellomrom e-postadressen som er knyttet til My Kaspersky-kontoen din. Den første slike sjekken utføres 48 timer etter installasjonen av Kaspersky. Ytterligere sjekker gjøres hver 24. time.

Datalekkasjekontroll for My Kaspersky-kontoen fungerer ikke hvis Kaspersky-programmet ikke er koblet til My Kaspersky, eller hvis passordet for My Kaspersky-kontoen ikke er angitt i programmet.

Slik aktiverer eller deaktiverer du Datalekkasjekontroll

Slik aktiverer eller deaktiverer du Kontosjekk:

1. Åpne hovedvinduet.
2. Velg delen **Personvern**.
3. I blokken **Datalekkasjekontroll** klikker du på **Søk etter lekkasjer**-knappen.
   Vinduet **Datalekkasjekontroll** vil da åpne.
4. Bruk bryteren for å aktivere eller deaktivere komponenten Datalekkasjekontroll.

Slik sjekker du om dataene dine kan bli offentlig tilgjengelig

Slik sjekker du om dataene dine kan bli offentlig tilgjengelige:

1. Åpne hovedvinduet.
2. Velg delen **Personvern**.
3. I blokken **Datalekkasjekontroll** klikker du på **Søk etter lekkasjer**-knappen.

   Vinduet **Datalekkasjekontroll** vil da åpne.
4. Skriv inn e-postadressen din i inntastingsfeltet og klikk på **Sjekk**.

   Kaspersky-programmet begynner å sjekke den angitte adressen. Hvis sjekken avslører at dataene dine kan være tilgjengelig for offentligheten, vil programmet varsle deg om dette og vise en liste over nettsteder hvor det kan ha oppstått en datalekkasje, datoen for mulig lekkasje og kategorien data som kan være offentlig tilgjengelig. Ved å klikke på en datakategorikobling vil du få anbefalinger om hvordan du kan minimere konsekvensene av en eventuell lekkasje av disse dataene.

   Kaspersky-programmet lar deg ikke bare sjekke dine egne data for mulige lekkasjer, men også fra andre brukerkontoer, for eksempel kontoer som tilhører venner og familie.

Slik oppretter du en liste over kontoer for automatisk sjekking

Slik oppretter du en liste over kontoer for automatisk sjekking:

1. Åpne hovedvinduet.
2. Velg delen **Personvern**.
3. I blokken **Datalekkasjekontroll** klikker du på **Søk etter lekkasjer**-knappen.

   Vinduet **Datalekkasjekontroll** vil da åpne.
4. I feltet **Sjekk flere kontoer** angir du e-postadressen til kontoen du vil legge til i listen for automatisk sjekking og klikker på knappen **Sjekk**.

   Kontoen du har lagt til vises i listen **Kontoer**.

Det kan hende at legge til kontoer i listen for automatisk sjekking ikke er tilgjengelig i området du bor i.

Privat surfing

I denne delen finner du informasjon om hvordan Kaspersky-programmet kan beskytte deg mot sporing av aktivitetene dine på nett.

Om Privat surfing

Kun tilgjengelig i Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Noen nettsteder bruker sporingstjenester for å samle inn informasjon om Internett-aktivitetene dine. Denne informasjonen blir deretter analysert og brukt med det formål å vise deg annonser.

Komponenten *Privat surfing* er utformet for å forhindre innsamling av informasjon om aktivitetene dine på nett.

I *oppdagelsesmodus* vil komponenten Privat surfing oppdage og telle antall forsøk på å samle inn data, og skrive denne informasjonen til en rapport. Oppdagelsesmodus er aktivert som standard, og datainnsamling er tillatt på alle nettsteder.

I *blokkeringsmodus* vil komponenten Privat surfing oppdage og blokkere forsøk på å samle inn data, og skrive informasjon om disse forsøkene til en rapport. I denne modusen blokkeres innsamling av data på alle nettsteder, unntatt:

- etter nettsteder lagt til som unntak
- etter nettstedene til Kaspersky og deres partnere
- etter nettsteder som kan slutte å fungere hvis du blokkerer sporingstjenester, i henhold til informasjon tilgjengelig for Kaspersky

Telleren for blokkerte forsøk på å samle inn data viser det totale antallet blokkeringer på hele nettstedet, avhengig av hvor mange sider som er åpne i nettleseren. Hvis én side er åpen i nettleseren, blir bare blokkerte forsøk på å samle inn data på denne siden på nettstedet talt. Hvis flere sider på samme nettsted er åpne i nettleseren, telles de blokkerte forsøkene på å samle inn data på alle sidene på nettstedet som er åpne i nettleseren.

Du kan administrere komponenten Privat surfing via grensesnittet i Kaspersky-programmet, eller ved hjelp av utvidelsen for Kaspersky Protection i nettleseren din.

Privat surfing har følgende begrensninger:

- Programmet blokkerer ikke sporingstjenestens innsamling av data for kategorien Sosiale nettverk mens du er på nettstedet til det aktuelle sosiale nettverket.
- Hvis det ikke kan fastslås hvilken webside forsøket på datainnsamling kom fra, vil Kaspersky-programmet verken blokkere forsøket på innsamling av data eller vise informasjon om det.
- Hvis websiden som forsøket på innsamling av data ble sendt fra kan fastslås, men ikke samsvarer med noen av websidene som er åpnet i nettleseren, bruker Kaspersky-programmet handlingen som er angitt i innstillingene til Privat surfing (blokkerer eller tillater innsamling av data). Programmet viser informasjon om forsøket på innsamling av data i rapporter, men inkluderer det ikke i statistikken som vises i vinduet Privat surfing, eller i nettleseren.

Komponenten er deaktivert som standard.

Blokkere innsamling av data

Slik blokkerer du innsamling av data:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. Velg komponenten **Privat surfing**, og klikk på ⚙ -ikonet.

Vinduet **Innstillinger for Privat surfing** vil da åpne.

4. Hvis komponenten er deaktivert, kan du aktivere den ved å sette bryteren øverst i vinduet til **På**.
5. Velg alternativet **Blokker innsamling av data**.

   Kaspersky-programmet vil blokkere forsøk på innsamling av data på alle nettsteder, bortsett fra unntak.
6. Slik blokkerer eller tillater du innsamling av data basert på kategoriene med sporingstjenester:

   a. Klikk på **Kategorier og unntak** for å åpne vinduet **Kategorier og unntak**.

   b. Som standard blokkeres innsamling av data for alle kategorier med sporingstjenester og på alle sosiale nettverk. Fjern kryssene i avmerkingsboksene ved siden av kategorier med sporingstjenester og sosiale nettverk du ønsker å tillate datainnsamling for.

Tillate innsamling av data på alle nettsteder

Slik tillater du innsamling av data på alle nettsteder:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. Velg komponenten **Privat surfing**, og klikk på -ikonet.

   Vinduet **Innstillinger for Privat surfing** vil da åpne.
4. Hvis komponenten er deaktivert, kan du aktivere den ved å sette bryteren øverst i vinduet til **På**.
5. Velg alternativet **Kun innhente statistikk**.

   Kaspersky-programmet oppdager og teller forsøk på å spore aktiviteten din på nett, uten å blokkere forsøkene. Du kan se resultatene av komponentens operasjon i rapporten.

Tillate innsamling av data som et unntak

Du kan tillate sporing av aktivitetene dine på bestemte nettsteder som et unntak.

Slik tillater du innsamling av data som et unntak:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. Velg komponenten **Privat surfing**, og klikk på -ikonet.

   Vinduet **Innstillinger for Privat surfing** vil da åpne.
4. Hvis komponenten er deaktivert, kan du aktivere den ved å sette bryteren øverst i vinduet til **På**.
5. Velg alternativet **Blokker innsamling av data**.

   Kaspersky-programmet vil blokkere forsøk på innsamling av data på alle nettsteder, bortsett fra unntak.

6. Som standard finnes det er unntak for å tillate datainnsamling på nettstedene til Kaspersky og deres partnere. Hvis du vil blokkere innsamling av data på disse nettstedene, deaktiverer du alternativet **Tillat innsamling av data på nettstedene til Kaspersky og deres partnere**.

7. Som standard finnes det et unntak for å tillate innsamling av data på nettsteder som kan slutte å fungere hvis du blokkerer innsamling av data, i henhold til informasjonen Kaspersky har tilgjengelig. Hvis du vil blokkere innsamling av data på disse nettstedene, deaktiverer du alternativet **Tillat innsamling av data på inkompatible nettsteder**.

   Kaspersky oppdaterer listen over inkompatible nettsteder etter hvert som kompatibilitetsproblemene løses.

8. Hvis du vil spesifisere dine egne unntak:

   a. Klikk på **Kategorier og unntak** for å åpne vinduet **Kategorier og unntak**.

   b. Klikk på **Unntak** for å åpne vinduet **Unntak for Privat surfing**.

   c. Klikk på **Legg til**.

   d. I vinduet som åpnes, skriver du inn adressen til nettstedet der du vil tillate sporing av aktiviteter. Deretter klikker du på **OK**.

      Det angitte nettstedet legges til i unntakslisten.

Du kan også tillate datainnsamling på et nettsted når det er åpnet i en nettleser.

Vis en rapport om forsøk på å samle inn dataene dine på Internett

Slik viser du en rapport om forsøk på å samle inn dataene dine på Internett:

1. Åpne hovedvinduet.

2. Gå til delen **Personvern**.

3. Velg komponenten **Privat surfing**, og klikk på -ikonet.

   Vinduet **Innstillinger for Privat surfing** vil da åpne.

   Hvis komponenten er deaktivert, kan du aktivere den ved å sette bryteren øverst i vinduet til **På**.

Vinduet viser en konsolidert rapport med informasjon om forsøk på å samle inn data om aktiviteten din på nett.

Du kan også vise rapporten om forsøket på datainnsamling i en nettleser eller i programytelsesrapporten.

Styre komponenten Privat surfing i en nettleser

Du kan styre komponenten Privat surfing direkte i nettleseren:

- Aktivere komponenten hvis den er deaktivert.

- Vise statistikk om oppdagede forsøk på datainnsamling.
- Gå til innstillingsvinduet i Privat surfing.
- Blokker eller tillat innsamling av data.

Hvis du vil styre komponenten Privat surfing i nettleseren,

Klikk på knappen **Kaspersky Protection** på verktøylinjen i nettleseren.

Menyen som åpnes, viser informasjon om komponentens operasjoner og kontroller.

Password Manager

Denne delen inneholder informasjon om hvordan du beskytter passordene dine.

Kontrollerer og lagrer passordene dine på en sikker måte

Kun tilgjengelig i Kaspersky Plus og Kaspersky Premium.

Hvis du er en aktiv Internettbruker, er du vant til å bruke mange ulike passord når du f.eks. besøker nettstedene til banker, sosiale nettverk og e-posttjenester. Det er upraktisk å bruke mange passord, ettersom du er nødt til å huske hvilket passord du brukte på hvilket nettsted. Dette fører ofte til at brukere tyr til den enkle løsningen, nemlig å bruke ett passord på ulike nettsteder. Dette er imidlertid ikke en sikker løsning. Hvis du bruker samme enkle passord på flere nettsteder, er det lettere for hackere å gjette eller fange opp passordet. Det kan bli dyrt for deg, hvis det dreier seg om passordet til en nettbankside.

Sjekk passordstyrken

Kaspersky-programmet sjekker sikkerheten til passordene du oppretter på Internett. Hvis passord ikke er sikre nok, kan Kaspersky hjelpe deg med å lage sterke passord og lagre dem på et trygt sted.

Beskytt mot bruk av de samme passordene

Når du angir et passord på et nettsted der et sikkert passord er spesielt viktig (f.eks. på et sosialt nettverk), ber Kaspersky-programmet deg om å aktivere beskyttelse mot bruk av identiske passord.

Hvis beskyttelse mot bruk av identiske passord er aktivert, vil Kaspersky-programmet sjekke om du allerede har brukt passordet du angir, på nettsteder innen følgende kategorier:

- Nettsteder for banker og betalingssystemer.
- Sosiale nettverk.
- E-posttjenester.

Hvis passordet du angir allerede er brukt på nettsteder i disse kategoriene, vil Kaspersky-programmet varsle deg og spørre om du vil opprette et nytt passord. Du kan velge nettstedkategoriene som bruk av identiske passord skal overvåkes for.

Sikker lagring av passord og dokumenter

Kaspersky Password Manager er utviklet for å sikre passordene og dokumentene dine. Den bruker et spesielt kryptert lager for å sikkert lagre den personlige informasjonen din: passord, identitetsdata, økonomisk eller medisinsk informasjon.

Du kan laste ned Kaspersky Password Manager fra vinduet i Kaspersky-programmet.

Slik laster du ned og installerer Kaspersky Password Manager

Hvis du vil laste ned Kaspersky Password Manager for å beskytte passordene dine,

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. I blokken **Passordsikkerhet** klikker du på **Last ned**-knappen.

   Installasjonspakken for Kaspersky Password Manager lastes ned på datamaskinen din. Hvis du vil installere Kaspersky Password Manager, følger du den standard fremgangsmåten for å installere programmer på datamaskinen.

Slik starter du Kaspersky Password Manager fra vinduet i Kaspersky-programmet

Slik kjører du Kaspersky Password Manager hvis det allerede er installert:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. I blokken **Passordsikkerhet** klikker du på **Start**-knappen.

   Vinduet Kaspersky Password Manager åpnes.

Se *hjelpesystemet for Kaspersky Password Manager* for å finne ut hvordan du bruker Kaspersky Password Manager.

Slik sjekker du sikkerheten til passordene dine

Kun tilgjengelig i Kaspersky Premium.

Internett-kontoene dine er i alvorlig fare hvis de passord som ikke er unike eller er svake (for eksempel qwerty eller 12345) og hvis passordene er basert på informasjon som er lett å gjette seg til eller få tak i (for eksempel navn på slektninger eller fødselsdatoer).

Kaspersky-programmet kan hjelpe deg med å raskt sjekke hvor komplekse passordene dine er, og om det samme passordet brukes for mer enn én konto.

Slik kontrollerer du passordsikkerheten:

1. Åpne hovedvinduet.
2. Velg delen **Personvern**.
3. Under **Passordsikkerhet** gjør du ett av følgende:
   - Klikk på **Last ned** hvis Kaspersky Password Manager ikke er installert enda. Knappen kan hete **Start** eller **Åpne** hvis Kaspersky Password Manager ikke er konfigurert, er utdatert eller er koblet til en My Kaspersky-konto som ikke stemmer overens med kontoen som Kaspersky-programmet er koblet til.

     Dette starter installasjonen av Kaspersky Password Manager. Følg instruksjonene i veiviseren.
   - Klikk på **Skann** hvis skanningen ikke er kjørt enda.
   - Klikk på **Detaljer** hvis skanningen allerede er kjørt.

Skanneresultatene vises under **Passordsikkerhet** og er gruppert etter sikkerhetskategorier.

Se *hjelpedelen for Kaspersky Password Manager* for å lære mer om passordskanning.

Konfigurere passordsikkerhet

Slik endrer du sikkerhetsinnstillinger for passord:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. I delen **Personverninnstillinger** velger du underkategorien **Sikkert datainput**.
4. Aktiver alternativet **Vis hint for hvordan du lager sterke passord** hvis du vil at Kaspersky-programmet skal kontrollere styrken til passordene du oppretter på nettsteder og gi deg anbefalinger for hvordan du oppretter sterke passord.

   Hvis du har installert Kaspersky Password Manager, vil varslingen anbefale deg å bruke et sterkt passord. Hvis Kaspersky Password Manager ikke er installert, anbefaler vi at du laster ned og installerer programmet, så du er sikker på at du alltid oppretter sterke passord.
5. Aktiver alternativet **Advar om bruk av samme passord på nettsteder** hvis du vil at Kaspersky-programmet skal sjekke om du har brukt passordet tidligere når du angir eller oppretter passord på nettstedene til banker, sosiale nettverk og e-posttjenester.
6. Klikk på koblingen **Velg nettstedkategorier** for å gå til vinduet **Nettstedkategorier**, hvis du vil velge hvilke nettstedkategorier identiske passord skal sjekkes for.
7. Aktiver alternativene for følgende kategorier:
   - **Internettbanker og betalingssystemer**. Når du oppretter eller angir et passord på Internett, vil Kaspersky-programmet sjekke om du har brukt dette passordet på nettstedene til banker eller betalingssystemer tidligere.
   - **Sosiale nettverk**. Når du oppretter eller angir et passord på Internett, vil Kaspersky-programmet sjekke om du har brukt dette passordet på sosiale nettverk tidligere.

- **E-posttjenester**. Når du oppretter eller angir et passord på Internett, vil Kaspersky-programmet sjekke om du har brukt dette passordet på e-posttjenester tidligere.

Safe Money

Denne delen gir instruksjoner om hvordan du kan beskytte finanstransaksjoner og nettkjøp med Kaspersky-programmet.

Om beskyttelse av finanstransaksjoner og nettkjøp

Kaspersky-programmet ber deg om å åpne nettstedene til banker og betalingssystemer i Beskyttet nettleser, slik at du kan beskytte konfidensielle data som du angir på disse nettstedene (for eksempel bankkortnumre og passord for nettbanker), og unngå at penger blir stjålet når du betaler på nettet.

Beskyttet nettleser er en spesiell nettlesermodus som beskytter dataene dine når du bruker nettstedene til banker og betalingssystemer. Beskyttet nettleser startes i et isolert miljø for å unngå at andre programmer setter inn sine koder i prosessen til Beskyttet nettleser. Kaspersky-programmet oppretter spesialprofiler for Mozilla Firefox og Google Chrome for å unngå at tredjeparts programtillegg påvirker funksjonaliteten til Beskyttet nettleser. Programmet påvirker ikke dataene som nettleserne lagrer i profilene som er opprettet for dem.

Hvis du bruker Chromium-basert Microsoft Edge, Google Chrome, Mozilla Firefox eller Internet Explorer, åpnes Beskyttet nettleser i et nytt vindu.

Programmet bruker Utvidelsen for Kaspersky Protection til flere av funksjonene i Beskyttet nettleser.

Nettlesere som ikke oppfyller programvarekravene kan ikke kjøre i Beskyttet nettleser-modus. I stedet for slike nettlesere vil enten Chromium-basert Microsoft Edge eller en annen nettleser i de konfigurerte programinnstillingene starte i Beskyttet nettleser-modus.

Det er umulig å kjøre beskyttet nettleser under følgende forhold:

- Det er ikke merket av for **Aktiver Selvforsvar** i vinduet **PC-ressursforbruk** i delen **Ytelsesinnstillinger**.
- Hvis Javascript er deaktivert i nettleseren.

Kjøre Beskyttet nettleser i Yandex Browser

Kaspersky-programmet støtter sikring av pengetransaksjonene dine i Yandex Browser, med noen begrensninger. For å kjøre Beskyttet nettleser vil programmet legge inn et spesielt skript på nettsiden (og i trafikken). Utvidelsen for Kaspersky Protection er ikke tilgjengelig. Komponentene Privat surfing og Anti-Banner kjører, men kan ikke konfigureres i Yandex Browser.

Funksjoner i Beskyttet nettleser

I modusen Beskyttet nettleser gir programmet beskyttelse mot følgende typer trusler:

- Uklarerte moduler. Programmet kjører en sjekk etter uklarerte moduler hver gang du besøker nettstedet til en bank eller et betalingssystem.

- Rotsett. Programmet skanner etter rotsett ved oppstart av Beskyttet nettleser.
- Ugyldige sertifikater for nettstedene til banker eller betalingssystemer. Programmet sjekker sertifikatene når du besøker nettstedet til en bank eller et betalingssystem. Sjekken utføres mot en database over kompromitterte sertifikater.

Beskyttet nettleser-status

Når du åpner et nettsted i Beskyttet nettleser, vil du se en ramme rundt margen i nettleservinduet. Fargen på rammen angir beskyttelsesstatusen.

Rammen rundt nettleservinduet kan ha følgende farger og betydning:

- Grønn ramme. Betyr at alle sjekker var vellykkede. Du kan fortsette å bruke Beskyttet nettleser.
- Gul ramme. Betyr at sjekkene har funnet sikkerhetsproblemer som må løses.

  Programmet kan registrere følgende trusler og sikkerhetsproblemer:

  - Uklarert modul. Datamaskinen må skannes og desinfiseres.
  - Rotsett. Datamaskinen må skannes og desinfiseres.
  - Ugyldig sertifikat for nettstedet til en bank eller et betalingssystem.

  Hvis du ikke fjerner de oppdagede truslene, kan vi ikke garantere sikkerheten av tilkoblingsøkten til nettstedet til banken eller betalingssystemet. Hendelser som gjelder oppstart og bruk av Beskyttet nettleser med redusert beskyttelse, registreres i hendelsesloggen i Windows.

Om beskyttelse mot skjermdumper

Kaspersky-programmet beskytter dataene dine ved å forhindre at spionprogrammer tar uautoriserte skjermdumper når du surfer på beskyttede nettsteder. Beskyttelse mot skjermdumper er aktivert som standard. Beskyttelse mot skjermbilder kjører selv om maskinvarevirtualisering er deaktivert.

Om databeskyttelse for utklippstavlen

Kaspersky-programmet blokkerer uautorisert tilgang til utklippstavlen når du foretar betalinger på nett, for å unngå at dataene blir stjålet av kriminelle. Denne typen blokkering er kun aktivert dersom et uklarert program prøver å få uautorisert tilgang til utklippstavlen. Hvis du kopierer data manuelt fra vinduet i et program til vinduet i et annet (for eksempel fra Notisblokk til et tekstredigeringsvindu), er tilgang til utklippstavlen tillatt.

Utklippstavlebeskyttelse kjører ikke hvis maskinvarevirtualisering er deaktivert på datamaskinen.

Hvis Beskyttet nettleser startes i operativsystemet Microsoft Windows 10, vil Kaspersky-programmet blokkere samhandling mellom universelle Windows-programmer og utklippstavlen.

Slik endrer du innstillinger for Safe Money

Slik konfigurerer du Safe Money:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Personverninnstillinger**.
4. Klikk på **Safe Money**.

   Vinduet viser innstillingene for komponenten Safe Money.
5. Aktiver Safe Money ved hjelp av bryteren øverst i vinduet.
6. I delen **Ved første tilgang til nettstedet til banker eller betalingssystemer** velger du handlingen som skal utføres av programmet når du først åpner nettstedet til en bank eller et betalingssystem i nettleseren:
   - Velg **Kjør Beskyttet nettleser** hvis du vil at programmet skal åpne nettstedet i Beskyttet nettleser.
   - Velg **Spør brukeren** hvis du vil at programmet skal spørre deg om du vil åpne nettstedet i Beskyttet nettleser når du besøker det.
   - Velg **Ikke kjør Beskyttet nettleser** hvis du ikke vil at programmet skal åpne nettstedet i Beskyttet nettleser.
7. I delen **Ekstra** åpner du rullegardinlisten **Hvis du vil fortsette til nettstedet fra vinduet Safe Money, bruker du** og velger nettleseren programmet vil kjøre i Beskyttet nettleser-modus når du besøker nettstedet til en bank eller et betalingssystem fra vinduet Safe Money.

   Du kan velge en av nettleserne installert på datamaskinen din, eller bruke den standard nettleseren til operativsystemet.

Slik konfigurerer du Safe Money for et bestemt nettsted

Slik konfigurerer du Safe Money for et bestemt nettsted:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. Velg delen **Safe Money** og klikk på **Vis nettsteder**.

   Vinduet **Safe Money** vil da åpne.
4. Klikk på koblingen **Legg til nettsted i Safe Money** for å åpne felter der du kan legge til nettstedinfo.
5. I feltet **Nettsted for Safe Money (URL)** angir du nettadressen til nettstedet som skal åpnes i Beskyttet nettleser.

   En nettstedadresse må innledes av prefikset for HTTPS-protokollen (for eksempel https://example.com). Dette prefikset settes inn som standard av den beskyttede nettleseren.
6. Velg handlingen du vil at Beskyttet nettleser skal utføre når du åpner nettstedet:

- Hvis du vil at nettstedet skal åpnes i Beskyttet nettleser hver gang du besøker det, merker du av for **Kjør Beskyttet nettleser**.
- Hvis du vil at Kaspersky-programmet skal be deg om å velge en handling hver gang nettstedet åpnes, merker du av for **Spør brukeren**.
- Hvis du vil deaktivere Safe Money for nettstedet, merker du av for **Ikke kjør Beskyttet nettleser**.

7. Klikk på koblingen **Legg til beskrivelse** for å åpne feltet **Beskrivelse**, og skriv inn et navn eller en beskrivelse for dette nettstedet.
8. Klikk på **Legg til**.

Nettstedet vises i listen.

Slik sender du en tilbakemelding om Safe Money

Du kan sende tilbakemeldinger til Kaspersky om Safe Money-komponentens virkemåte eller rapportere et problem med denne komponenten.

Slik sender du tilbakemelding

Slik sender du tilbakemeldinger om operasjonen til komponenten Safe Money.

1. Åpne hovedvinduet.
2. Gå til delen **Sikkerhet**.
3. Velg delen **Safe Money** og klikk på **Vis nettsteder**.
   Vinduet **Safe Money** vil da åpne.
4. Klikk på **Send tilbakemelding** for å åpne et vindu der du kan legge inn en tilbakemelding om Safe Money-komponentens ytelse.
5. Vennligst vurder Safe Money på en skala fra 1 til 5 ved å velge 1 til 5 stjerner.
6. Hvis du vil legge ved en kommentar til tilbakemeldingen din, skriver du inn teksten i feltet **Detaljer**.
7. Klikk på **Send**.

Slik rapporterer du et problem

Slik rapporterer du et problem med Beskyttet nettleser:

1. Klikk på koblingen **Rapporter et problem** i popup-vinduet i den nederste delen av Beskyttet Nettleser.

   I vinduet som åpnes, kan du rapportere et problem med Safe Money.

2. I nedtrekkslisten **Problem** velger du elementet som beskriver problemet best:

   - **Jeg bruker det ikke**. Velg dette elementet hvis du ikke bruker Safe Money eller har besluttet å avvelge bruk av Safe Money.
   - **Nettstedet åpnes for tregt**. Velg dette elementet hvis det tar lengre tid å åpne nettstedet enn det tar i en vanlig nettleser.
   - **Beskyttet nettleser starter når det ikke trengs**. Velg dette elementet hvis nettsteder som ikke krever bruk av Safe Money, åpnes i Beskyttet nettleser.
   - **Nettstedet kan ikke autoriseres**. Velg dette elementet hvis det oppstår feil under autorisasjonsforsøk på et nettsted åpnet i Beskyttet nettleser.
   - **Nettstedet vises feil eller åpnes ikke**. Velg dette elementet hvis nettsteder ikke åpnes i Beskyttet nettleser eller vises med feil eller forvrengninger.
   - **Feil ved verifisering av nettstedets sertifikat**. Velg dette elementet hvis feilmeldinger vises under valideringen av nettstedssertifikater.
   - **Kunne ikke ta et skjermbilde mens Beskyttet nettleser kjører**. Velg dette elementet hvis skjermbilder ikke opprettes i Beskyttet nettleser.
   - **Feil under inntasting eller innliming fra tastaturet eller utklippstavlen**. Velg dette elementet hvis det oppstår feil under inntasting av data i Beskyttet nettleser.
   - **En nettside åpnet i Beskyttet nettleser kan ikke skrives ut**. Velg dette elementet hvis du ikke kan skrive ut en åpen side på et nettsted.
   - **Det vises en melding som advarer om viktige operativsystemoppdateringer som ikke er installert**. Velg dette elementet hvis «Viktige systemoppdateringer er ikke installert» vises når du kjører Beskyttet nettleser.
   - **En annen nettleser kjører som Beskyttet nettleser**. Velg dette elementet hvis Beskyttet nettleser åpnes i en annen nettleser enn den du starter den med.
   - **Feil under bruk**. Velg dette elementet hvis Beskyttet nettleser har returnert en feil.
   - **Annet**. Velg dette elementet hvis problemet du opplever ikke dekkes av andre elementer.

3. For å sende ytterligere informasjon om problemet til Kaspersky kan du skrive inn beskrivelsen i tekstfeltet **Detaljer**.

4. Klikk på knappen **Send**.

Hvis Kaspersky-programmet ikke kan sende tilbakemeldingen (for eksempel fordi du ikke har internettforbindelse), lagres tilbakemeldingen på datamaskinen. Den lagrede tilbakemeldingen vil være synlig i 30 dager.

Du kan sende tilbakemeldinger om operasjonen til komponenten Safe Money opptil ti ganger hver dag.

Du kan også sende tilbakemeldinger etter at komponenten Safe Money er deaktivert. Etter at komponenten er deaktivert, kan du sende tilbakemeldinger én gang i måneden.

Webkamera og mikrofonkontroll

Denne delen inneholder informasjon om hvordan du forhindrer at noen spionerer på deg gjennom webkameraet og avlytting gjennom mikrofonen.

Kun tilgjengelig i Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Om programmers tilgang til webkameraet og mikrofonen

Inntrengere kan forsøke å spionere på deg ved å bruke webkameraet ditt, eller å avlytte deg ved å få tilgang til mikrofonen din. Kaspersky-programmet beskytter webkameraet og mikrofonen mot uautorisert tilgang hvis komponenten Webkamera og mikrofonkontroll er aktivert. I komponentens innstillinger kan du blokkere alle programmers tilgang til webkameraet og mikrofonen, eller be om å bli varslet når en program prøver å få tilgang til webkameraet eller mikrofonen din.

Hvis komponenten er aktivert, men tilgangen til webkameraet og mikrofonen ikke er fullstendig blokkert, vil tilgang bli gitt eller nektet basert på hvilken klareringsgruppe det aktuelle programmet tilhører. Tilgang er blokkert for programmer i gruppene Høyt begrenset eller Uklarert.

Med vinduet Inntrengningsbeskyttelse kan du tillate tilgang til webkameraet eller mikrofonen for programmer som er inkludert i gruppene Høyt begrenset og Uklarert. Hvis et program fra gruppen Lavt begrenset prøver å få tilgang til webkameraet eller mikrofonen, blokkerer Kaspersky-programmet tilgangen og varsler deg hvis du har konfigurert varsler i komponentinnstillingene.

I rullegardinlisten på varlingen kan du blokkere programtilgang til tilgang til webkameraet eller mikrofonen, eller gå til tilgangsinnstillingene. Varslingen vises ikke hvis enkelte programmer kjører i fullskjermsmodus på datamaskinen

I rullegardinlisten i varslingen kan du også velge å skjule varslinger eller gå videre til konfigurasjon av innstillinger for visning av varslinger.

Slik administrerer Kaspersky webkameraet

Som standard gir Kaspersky-programmet webkameraet tilgang til programmer som krever din tillatelse, i tilfeller der programmets grafiske brukergrensesnitt lastes, utlastes eller ikke svarer, og du ikke kan tillate tilgang manuelt.

Beskyttelse av webkameratilgang har følgende funksjoner og begrensninger:

- Kaspersky-programmet begrenser video- og øyeblikksbilder som er et resultat av behandling av data fra webkameraet.
- Kaspersky-programmet kontrollerer lydsignaler hvis dette er en del av videostrømmen fra webkameraet.
- Kaspersky-programmet kontrollerer kun webkameraer som er tilkoblet via USB eller IEEE1394, og som er oppført som bildeenheter i Windows Enhetsbehandling.

Klikk på denne koblingen for å vise en liste over støttede webkameraer.

Komponenten Inntrengningsbeskyttelse må være aktivert for at du skal kunne aktivere beskyttelse mot uautorisert tilgang til webkameraet.

Webkamerabeskyttelse har begrensninger hvis programmet ble installert i Microsoft Windows 10 Anniversary Update (RedStone 1).

Slik administrerer Kaspersky mikrofonen

Beskyttelse av mikrofonen har følgende spesialfunksjoner:

- Komponenten Inntrengningsbeskyttelse må være aktivert for at funksjonen skal fungere.
- Etter at innstillingene for programmers tilgang til lydopptaksenheter er endret (for eksempel hvis programmet ikke har tillatelse til å motta lyddataflyten i innstillingene i vinduet Inntrengningsbeskyttelse), må dette programmet startes på nytt for å hindre at det mottar lyddataflyten.
- Kaspersky-programmet beskytter bare tilgang til innebygde mikrofoner og eksterne mikrofoner. Andre enheter for lyddataflyt støttes ikke.
- Kaspersky-programmet tillater at et program mottar en lyddataflyt uten å vise varslinger, hvis programmet begynte å motta lyddataflyten før Kaspersky-programmet ble startet, eller hvis du plasserte programmet i gruppene Uklarert eller Høyt begrenset etter at programmet begynte å motta lyddataflyten.

Kaspersky-programmet garanterer ikke beskyttelse av lyddataflyter fra enheter som f.eks. digitale speilrefleksskameraer (DSLR), videokameraer, og actionkameraer.

Slik endrer du innstillinger for programmers tilgang til webkameraet eller mikrofonen

Slik endrer du innstillinger for programmers tilgang til webkameraet eller mikrofonen:

1. Åpne hovedvinduet.

2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.

3. I delen **Personverninnstillinger** velger du komponenten **Kontroll av webkamera og mikrofon**.

4. Under **Webkamera-innstillinger** velger du en av følgende handlinger:

   - **Blokker tilgang til webkameraet for alle programmer**. Webkameratilgang er blokkert for alle programmer som er installert på datamaskinen din.
   - **Varsle hvis et program bruker webkameraet**. Programmer som har tilgang som standard vil få tilgang til webkameraet. Det vises en varsling som informerer brukeren om at et bestemt program bruker webkameraet.

5. Under **Mikrofoninnstillinger** velger du en av følgende handlinger:

   - **Blokker tilgang til mikrofonen for alle programmer**. Mikrofontilgang er blokkert for alle programmer som er installert på datamaskinen din.
   - **Varsle hvis et program bruker mikrofonen**. Programmer som har tilgang som standard vil få tilgang til mikrofonen. Det vises en varsling som informerer brukeren om at et bestemt program bruker mikrofonen.

Slik gir eller blokkerer du tilgang til webkameraet for et bestemt program

Slik gir eller blokkerer du tilgang til webkameraet for et program

1. Åpne hovedvinduet.
2. Gå til delen **Sikkerhet**.
3. Aktiver komponenten **Inntrengningsbeskyttelse**.
4. Klikk på **Behandle programmer** for å åpne vinduet **Behandle programmer**.
5. Velg programmet du vil tillate tilgang til lydopptaksenheter for, i listen. Dobbeltklikk på programmet for å åpne vinduet **Programregler**.
6. I vinduet **Programregler** går du til kategorien **Rettigheter**.
7. Fra listen over rettighetskategorier velger du **Endring av operativsystemet → Mistenkelige endringer i operativsystemet**.
8. Velg **Tilgang til webkamera**.
9. I kolonnen **Handling** velger du **Tillat** eller **Nekt**.
10. Klikk på **Lagre**.

Hvis du velger **Blokker tilgang til webkameraet for alle programmer**, blokkeres programmenes tilgang til webkameraet uavhengig av klareringsgruppen og manuelt konfigurerte tillatelser.

Slik gir eller blokkerer du tilgang til mikrofonen for et bestemt program

Slik gir eller blokkerer du tilgang til mikrofonen for et program

1. Åpne hovedvinduet.
2. Gå til delen **Sikkerhet**.
3. Aktiver komponenten **Inntrengningsbeskyttelse**.
4. Klikk på **Behandle programmer** for å åpne vinduet **Behandle programmer**.
5. I listen velger du programmet du vil gi tilgang til mikrofonen for, og dobbeltklikker for å åpne vinduet **Programregler**.
6. I vinduet **Programregler** går du til kategorien **Rettigheter**.
7. Fra listen over rettighetskategorier velger du **Endring av operativsystemet** → **Mistenkelige endringer i operativsystemet** → **Få tilgang til lydopptaksenheter**.
8. I kolonnen **Handling** velger du **Tillat** eller **Nekt**.
9. Du kan velge å motta varsler når programmer tillates eller nektes tilgang til lydstrømmen, ved å gå til kolonnen **Handling**, klikk på ikonet og velge **Logg hendelser**.
10. Klikk på **Lagre**.

Hvis du velger **Blokker tilgang for alle programmer**, blokkeres programmenes tilgang til mikrofonen uavhengig av klareringsgruppen og manuelt konfigurerte tillatelser.

Stalkerware-deteksjon

Kriminelle kan bruke enkelte legitime programmer til å stjele de personlige dataene dine og spionere på deg. De fleste av disse programmene er nyttige, og mange har nytte av å bruke dem. Disse programmene inkluderer IRC-klienter, automatiske oppringere, filnedlastere, systemaktivitetsovervåkere, passordbehandlingsverktøy, FTP, HTTP eller telnett-servere.

Hvis kriminelle får tilgang til disse programmene på datamaskinen din, eller klarer å distribuere dem der i det skjulte, vil de kunne bruke noen av funksjonene til å stjele de personlige dataene dine eller begå andre ulovlige handlinger.

Du kan lese om ulike typer stalkerware nedenfor.

Type	Navn	Beskrivelse
Client-IRC	IRC-klienter	Folk installerer disse programmene for å kommunisere med hverandre i Internet Relay Chats (IRC). Kriminelle kan bruke disse programmene til å spre skadelig programvare.
Dialer	Automatiske oppringere	Kan opprette telefonforbindelser i det skjulte over et modem.

Downloader	Nedlastere	Kan laste ned filer i det skjulte fra nettsider.
Monitor	Overvåker programmer	Gjør det mulig å overvåke aktiviteten til datamaskinen de er installert på (sporer hvilke programmer som kjører, og hvordan de utveksler data med programmer på andre datamaskiner).
PSWTool	Verktøy for gjenoppretting av passord	Gjør det mulig for brukerne å se og gjenopprette glemte passord. Kriminelle distribuerer disse programmene i det skjulte på folks datamaskiner for samme formål.
RemoteAdmin	Fjernstyringsverktøy	Brukes ofte av systemadministratorer for å få tilgang til eksterne datamaskiners grensesnitt for å overvåke og kontrollere dem. Kriminelle distribuerer disse programmene i det skjulte på folks datamaskiner for samme formål, for å spionere på eksterne datamaskiner og fjernstyre dem. Legitime fjernstyringsverktøy er forskjellige fra bakdører (fjernstyringstrojanere). Bakdører kan infiltrere et system og installere seg der selv, uten brukerens tillatelse, noe legitime programmer ikke kan.
Server-FTP	FTP-server	Fungerer som FTP-servere. Kriminelle kan distribuere dem på datamaskinen din for å fjernstyre den ved hjelp av FTP-protokollen.
Server-Proxy	Proxy-servere	Fungerer som proxy-servere. Kriminelle distribuerer dem på en datamaskin for å bruke den til å sende ut spam.
Server-Telnet	Telnet-servere	Fungerer som Telnet-servere. Kriminelle distribuerer dem på en datamaskin for å fjernstyre den ved hjelp av Telnet-protokollen.
Server-Web	Webservere	Fungerer som webservere. Kriminelle kan distribuere dem på datamaskinen din for å fjernstyre den ved hjelp av HTTP-protokollen.
RiskTool	Lokale verktøy	De gir brukere flere muligheter til å styre datamaskinene sine (slik at de kan skjule filer eller aktive programvinduer, eller lukke aktive prosesser).
NetTool	Nettverksverktøy	De gir brukerne av datamaskiner som de er installert på, flere muligheter til å samhandle med andre datamaskiner på nettverket (starte eksterne datamaskiner på nytt, finne åpne porter, starte programmer installert på disse datamaskinene).
Client-P2P	P2P-nettverksklienter	Gjør det mulig for folk å bruke P2P-nettverk (node-til-node). Kriminelle kan bruke dem til å spre skadelig programvare.
Client-SMTP	SMTP-klienter	Kan sende e-poster i det skjulte. Kriminelle distribuerer dem på en datamaskin for å bruke den til å sende ut spam.
WebToolbar	Nettverktøylinjer	Legger til søkemotorverktøylinjer i grensesnittet til andre programmer.
FraudTool	Svindelprogrammer	Etterligner andre programmer. For eksempel finnes det antivirus-svindelprogrammer som viser varsler om at de oppdager skadelig programvare på en datamaskin, selv om de faktisk verken finner, renser eller reparerer noe.

Aktiver beskyttelse mot stalkerware, så advarer vi deg om alle forsøk på å få tilgang til posisjonsdata, meldinger eller andre personlige data.

Du kan også aktivere stalkerware-beskyttelse i vinduet **Innstillinger for trusler og unntak** ved å merke av i boksen **Finn annen programvare som kriminelle kan bruke til å skade datamaskinen eller dine personlige data**.

Anti-Banner

I denne delen finner du informasjon om hvordan Kaspersky kan beskytte deg mot annonsebannere på Internett.

Om Anti-Banner

Kun tilgjengelig i Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Komponenten Anti-Banner er utviklet for å gi beskyttelse mot bannere når du surfer på nettet. Anti-Banner blokkerer bannere på nettstedene du åpner, samt i grensesnittene til bestemte programmer. Anti-Banner blokkerer bannere fra listen over ukjente bannere, som er bygd inn i databasene til Kaspersky-programmet. Du kan administrere blokkering av bannere, enten i grensesnittet til Kaspersky-programmet eller direkte i nettleseren.

Som standard tillates bannere på nettsteder fra listen over **Kasperskys nettsteder**. Denne listen kompileres av Kasperskys eksperter og inkluderer nettstedene til Kaspersky og deres partnere som inneholder Kaspersky-annonser. Du kan vise denne listen eller deaktivere bruk av den hvis du ser det som nødvendig å blokkere bannere på nettstedene til Kaspersky og dets partnere.

Telleren for blokkerte bannere viser det totale antallet blokkeringer på hele nettstedet, avhengig av hvor mange sider som er åpne i nettleseren. Hvis én side er åpen i nettleseren, blir bare blokkeringer på denne siden på nettstedet talt. Hvis flere sider på samme nettsted er åpne i nettleseren, telles de blokkerte bannerne på alle sidene på nettstedet som er åpne i nettleseren.

Informasjon om funksjonen til Anti-Banner er tilgjengelig i rapporter.

Følgende begrensninger gjelder for Anti-Banner:

- Enkelte nettsider oppdager at annonser på sidene deres er blokkert, og viser ikke innholdet før brukeren slår av annonseblokkeringen. Hvis du vil se innholdet på slike sider, må du legge til adressene i unntakslisten.
- Hvis det ikke kan fastslås hvilken webside banneret er på, vil Kaspersky-programmet verken blokkere eller vise informasjon om banneret.
- Hvis det kan fastslås hvilken webside banneret er på, men websiden ikke samsvarer med noen av websidene som er åpnet i nettleseren, vil Kaspersky-programmet blokkere banneret eller tillate at banneret vises, avhengig av informasjonen som har blitt fastslått. Programmet viser informasjon om dette banneret i rapporter, men inkluderer ikke denne informasjonen i statistikken for Privat surfing i nettleseren.
- Statistikk som vises for Anti-Banner i nettleseren kan inkludere bannere som ble blokkert forrige gang websidene ble lastet inn, inkludert bannere som har blitt blokkert tidligere og som lastes inn på nytt.
- Statistikken for Anti-Banner, som vises i nettleseren, inkluderer ikke bannere som ble blokkert i dynamisk innhold på en side etter at et nettsted har blitt låst.

Slik aktiverer du komponenten Anti-Banner

Komponenten Anti-Banner er deaktivert som standard. Du kan aktivere den via grensesnittet i Kaspersky-programmet, eller ved hjelp av utvidelsen for Kaspersky Protection i nettleseren din.

Slik aktiverer du Anti-Banner i Kaspersky-programmets grensesnitt

Slik aktiverer du Anti-Banner i Kaspersky-programmets grensesnitt:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Personverninnstillinger**.
4. Aktiver komponenten Anti-Banner.
   Vinduet **Innstillinger for Anti-Banner** vil da åpne.
5. Aktiver komponenten ved hjelp av bryteren øverst i vinduet.

Slik aktiverer du Anti-Banner i nettleservinduet

Slik aktiverer du Anti-Banner i nettleservinduet:

1. Klikk på knappen **Kaspersky Protection** på verktøylinjen i nettleseren.
2. Klikk på knappen **Aktiver** i rullegardinmenyen i delen **Anti-Banner**.

Etter at du har aktivert eller deaktivert Anti-Banner, må du laste inn nettsiden i nettleseren på nytt for at endringene skal tre i kraft.

Blokkere bannere

Anti-Banner blokkerer nettstedbannere fra listen over ukjente bannere, som er bygd inn i databasene til Kaspersky-programmet. Hvis et banner vises på en webside selv om Anti-Banner kjører, kan dette bety at banneret ikke er i listen over ukjente bannere. Du kan blokkere visningen av dette banneret manuelt.

Hvis du vil blokkere et banner, må du legge det til i listen over blokkerte bannere. Dette kan du gjøre direkte på websiden, eller i grensesnittet til Kaspersky-programmet.

Du kan ikke blokkere et banner hvis det er på et nettsted som er i listen over nettsteder med tillatte bannere.

Slik blokkerer du et banner på en webside

Slik blokkerer du et banner på en webside:

1. Pass på at utvidelsen for Kaspersky Protection er installert og aktivert i nettleseren.
2. Hvis Anti-Banner er deaktivert, aktiverer du det:
   a. Klikk på knappen **Kaspersky Protection** på verktøylinjen i nettleseren.
   b. Klikk på knappen **Aktiver** i rullegardinmenyen i delen **Anti-Banner**.
3. Hold markøren over banneret du ønsker å blokkere, og høyreklikk.
4. Velg **Legg til i Anti-Banner** i hurtigmenyen som åpnes.
   Vinduet **Legg til blokkert banner** åpnes.
5. I vinduet **Legg til blokkert banner** klikker du på **Legg til**.
   Bannerets URL-adresse legges til i listen over blokkerte bannere.
6. Oppdater websiden i nettleseren for å fjerne visning av banneret.

Banneret vil ikke vises neste gang du går til denne websiden.

Slik blokkerer du et banner i Kaspersky-programmet:

Slik blokkerer du et banner i Kaspersky-programmet:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Personverninnstillinger**.
4. Aktiver komponenten Anti-Banner.

   Vinduet **Innstillinger for Anti-Banner** vil da åpne.
5. Aktiver komponenten Anti-Banner ved hjelp av bryteren øverst i vinduet.
6. I vinduet **Innstillinger for Anti-Banner** klikker du på lenken **Blokkerte bannere** for å åpne vinduet **Blokkerte bannere**.
7. I vinduet **Blokkerte bannere** klikker du på **Legg til**-knappen.
8. I vinduet som åpnes, angir du bannerets adresse eller adressemaske i feltet **Nettadressemaske (URL)**.
9. Angi **Aktiv** som status for dette banneret.
10. Klikk på **OK**.

    Kaspersky-programmet vil blokkere det angitte banneret.

Tillate bannere

Du kan tillate ett enkelt banner eller alle bannere på et nettsted du spesifiserer.

Slik tillater du ett enkelt banner

Slik tillater du ett enkelt banner:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Personverninnstillinger**.
4. Aktiver komponenten Anti-Banner.

   Vinduet **Innstillinger for Anti-Banner** vil da åpne.
5. Aktiver komponenten Anti-Banner ved hjelp av bryteren øverst i vinduet.
6. I vinduet **Innstillinger for Anti-Banner** klikker du på lenken **Nettsteder med tillatte bannere** for å åpne vinduet **Nettsteder med tillatte bannere**.
7. I vinduet **Nettsteder med tillatte bannere** klikker du på **Legg til**-knappen.
8. I vinduet som åpnes, angir du bannerets adresse eller adressemaske i feltet **Nettsted**.
9. Velg statusen **Aktiv**.
10. Klikk på **OK**.

Programmet vil ikke blokkere det spesifiserte banneret.

Hvis et banner ble lagt til på listen med tillatte bannere, men banneret er inni en annonseblokkering med egenskaper som gjør at det blokkeres av Anti-Banner på et nettsted, vil både banneret og annonseblokkeringen bli blokkert.

Slik tillater du alle bannere på et nettsted

Slik tillater du alle bannere på et nettsted:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Personverninnstillinger**.
4. Aktiver komponenten Anti-Banner.
   Vinduet **Innstillinger for Anti-Banner** vil da åpne.
5. Aktiver komponenten Anti-Banner ved hjelp av bryteren øverst i vinduet.
6. I vinduet **Innstillinger for Anti-Banner** klikker du på lenken **Nettsteder med tillatte bannere** for å åpne vinduet **Nettsteder med tillatte bannere**.
7. I vinduet **Nettsteder med tillatte bannere** klikker du på **Legg til**-knappen.
8. Skriv inn URL-adressen, for eksempel `example.com`, i feltet **Nettsted** i vinduet som åpnes.
9. Velg statusen **Aktiv**.
10. Klikk på **OK**.

    Nettstedet vil bli lagt til i listen over nettsteder med tillatte bannere. Kaspersky blokkerer ikke bannere på nettsteder fra denne listen, selv om et banner er lagt til i listen med blokkerte bannere.

Slik konfigurerer du Anti-Banner-filtre

Slik konfigurerer du Anti-Banner-filtre:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Personverninnstillinger**.
4. Aktiver komponenten Anti-Banner.
   Vinduet **Innstillinger for Anti-Banner** vil da åpne.
5. Aktiver komponenten Anti-Banner ved hjelp av bryteren øverst i vinduet.
6. Klikk på **Liste over filtre** for å åpne vinduet **Liste over filtre**.
7. I vinduet **Liste over filtre** kan du konfigurere filtrene etter behov:

- **Anbefalt**. Denne gruppen inneholder det generelle filter- og språkfilteret som svarer til din region. Disse filtrene er aktivert som standard.
- **Tematisk**. Denne gruppen inneholder to filtre:
  - **Sosiale medier**. Aktiver dette filteret hvis du vil blokkere elementer som like- og dele-knappene på nettsteder for sosiale nettverk.
  - **Irritasjonsmomenter**. Aktiver dette filteret hvis du vil blokkere popup-meldinger, vinduer og andre elementer som ikke tilhører det aktuelle nettstedet.
- **Språkspesifikt**. I denne gruppen av filtre kan du velge et språk. Programmet vil blokkere bannere på nettsteder på det angitte språket.

Slik administrerer du Anti-Banner i nettleseren

Du kan administrere komponenten Anti-Banner rett fra nettleseren ved hjelp av utvidelsen for Kaspersky Protection:

Utvidelsen for Kaspersky Protection lar deg utføre følgende handlinger:

- Aktivere og deaktivere komponenten
- Vis statistikk for blokkerte bannere
- Gå til vinduet Innstillinger for Anti-Banner
- Vis informasjon som forteller deg om bannere skal blokkeres på et nettsted som åpnes i nettleseren, og behandle visning av bannere på et nettsted

Slik administrerer du komponenten Anti-Banner via utvidelsen for Kaspersky Protection

Slik administrerer du komponenten Anti-Banner via utvidelsen for Kaspersky Protection:

Klikk på knappen **Kaspersky Protection** på verktøylinjen i nettleseren.

Menyen som åpnes, viser informasjon om komponentens operasjoner og kontroller.

Blokkering av installasjon av uønskede programmer

Noen ganger installerer du et program, og finner ut senere at det samtidig ble installert flere programmer du ikke har bedt om. Høres det kjent ut? Disse uønskede programmene installeres uten at du vet det, og kan bombardere deg med annonser eller til og med endre hvilken nettleser du bruker som standard.

Aktiver **Blokkering av installasjon av uønskede programmer** i delen **Personvern** for å glemme dette problemet en gang for alle. Blokkering av installasjon av uønskede programmer fjerner automatisk merket i avmerkingsboksene for eventuelle tilleggsprogrammer som foreslås, slik at du slipper å fjerne merket for dem manuelt.

Du kan også aktivere Blokkering av installasjon av uønskede programmer i vinduet med innstillinger for Application Manager.

Merk av for alternativet **Deaktiver avmerkingsboksene for installasjon av tilleggsprogrammer når du installerer programmer. Advar mot alle forsøk på å installere tilleggsprogrammer** for å gjøre dette.

Blokkering av installasjon av uønskede programmer støtter kanskje ikke alle programmer som kan installeres. Hvis et installerbart program ikke støttes, er det umulig å blokkere installasjonen av uønskede programmer. Ekspertene våre utvider listen over støttede installerbare programmer kontinuerlig.

Slik endrer du innstillinger for Application Manager

Kun tilgjengelig i Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Slik endrer du innstillinger for Application Manager:

1. Åpne hovedvinduet.
2. Velg delen **Personvern**.
3. I blokken **Blokkering av installasjon av uønskede programmer** klikker du på .

   Dette tar deg til vinduet **Innstillinger for Application Manager**.
4. I innstillingsgruppen **Blokkering av installasjon av uønskede programmer** velger du avmerkingsboksen **Deaktiver avmerkingsboksene for installasjon av tilleggsprogrammer når du installerer programmer. Advar mot alle forsøk på å installere tilleggsprogrammer** for å blokkere installasjon av ekstra programvare ved installasjon av nye programmer. Hvis uønskede operasjoner forhindres under installasjon av det nye programmet, vil Kaspersky-programmet varsle deg om dette.

   Hvis alternativet **Deaktiver avmerkingsboksene for installasjon av tilleggsprogrammer når du installerer programmer. Advar mot alle forsøk på å installere tilleggsprogrammer** ble deaktivert etter at du begynte å installere et bestemt program, fortsetter Blokkering av installasjon av uønskede programmer å kjøre under den nåværende installasjonen. Avmerkingsboksene ved siden av tilbud om installasjon av tilleggsprogrammer deaktiveres, og tilleggsprogrammene installeres ikke. Denne funksjonaliteten deaktiveres under neste installasjon. Ekstraprogrammer installeres sammen med hovedprogrammet.
5. Merk av for alternativet **Ikke vis installasjonstrinn som kan inneholde reklame og tilbyr å installere tilleggsprogrammer** for å blokkere visning av installasjonstrinn med annonser under installasjon av ny programvare på datamaskinen. Hvis slike installasjonstrinn blir fjernet, vil Kaspersky-programmet varsle deg om dette.

Fjerning av annonseprogrammer

Får du mange irriterende annonser? Kaspersky-programmet kan slette programmer som viser annonser i nettleserne og på skrivebordet fra datamaskinen din. I tillegg til annonseprogrammer, vil vi også fjerne alle automatiske oppringere og mistenkelige pakker som kan inneholde virus og andre trusler. Aktiver **Fjerning av annonseprogrammer** for å aldri se de irriterende annonsene igjen.

Slik fjerner du annonseprogrammer:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. Aktiver **Fjerning av annonseprogrammer**.

Hemmelig hvelv

Denne delen beskriver hvordan du beskytter data med hemmelige hvelv.

Om Hemmelig hvelv

Kun tilgjengelig i Kaspersky Plus og Kaspersky Premium.

Hemmelige hvelv er utformet for å beskytte konfidensielle data mot uautorisert tilgang. Et *hemmelig hvelv* er et lager på datamaskinen som du kan låse og åpne med et passord som bare du kjenner. Du må angi passordet for å kunne endre filene som er lagret i et hemmelig hvelv. Hvis du har angitt feil passord 10 ganger på rad, vil tilgangen til det hemmelige hvelvet være blokkert i én time.

Hvis du mister eller glemmer passordet, kan du ikke gjenopprette dataene dine.

Kaspersky-programmet oppretter hemmelig hvelv med datakrypteringsalgoritmen AES XTS, som har en effektiv nøkkellengde på 56 biter.

> Hvis FAT32-filsystemet brukes på datamaskinen din, kan du opprette hemmelige hvelvet som ikke er større enn 4 GB.

Slik flytter du filer til et hemmelig hvelv

Slik flytter du filer til et hemmelig hvelv:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. Gjør ett av følgende i vinduet **Hemmelig hvelv**:

Hvis du enda ikke har hemmelig hvelv

1. Klikk på **Opprett hvelv**.
2. I vinduet **Hemmelig hvelv** klikker du på **Legg til** og velger filer i Windows Utforsker, eller drar og slipper filer til vinduet i Kaspersky-programmet.

   De valgte filene vises i vinduet **Hemmelig hvelv**.
3. Klikk på **Fortsett**.
4. Angi navnet på det hemmelige hvelvet og angi hvelvets plassering, eller bruk standardverdiene i disse innstillingene.
5. Angi størrelsen på det hemmelige hvelvet.
6. Hvis du vil ha rask tilgang til datahvelvet, merker du av for alternativet **Lag en skrivebordssnarvei for hemmelig hvelv**.
7. Klikk på **Fortsett**.
8. Fyll ut feltene **Passord for å åpne det hemmelige hvelvet** og **Bekreft passord**, og klikk på **Fortsett**.
9. Velg hva som skal gjøres med kildekopiene til filene utenfor det hemmelige hvelvet:
   - Hvis du vil slette kildekopiene utenfor det hemmelige hvelvet, klikker du på **Slett**.
   - Hvis du vil beholde kildekopiene utenfor det hemmelige hvelvet, klikker du på **Hopp over**.
10. Klikk på **Fullført**.

    Listen over hemmelige hvelv viser det hemmelige hvelvet du nettopp opprettet.
11. Hvis du vil låse det hemmelige hvelvet, klikker du på **Lås**.

    Du må angi et passord for å få tilgang til data i et låst hemmelig hvelv.

Hvis du allerede har et hemmelig hvelv

1. Klikk på **Jeg har allerede et hemmelig hvelv** for å åpne vinduet **Hemmelig hvelv**.
2. I vinduet **Hemmelig hvelv** velger du den hemmelige mappen og klikker på **Lås opp**.
3. Angi passordet, og klikk deretter på **Åpne i Windows Utforsker**.

   Dette åpner det hemmelige hvelvet i Windows Utforsker.
4. Flytt filene dine til det hemmelige hvelvet.
5. Lukk vinduet i Windows Utforsker.
6. I grensesnittet til Kaspersky-programmet går du til vinduet **Hemmelig hvelv** og klikker på **Lås**.

Når du legger til filer med identiske navn i hemmelige hvelvet, der den eneste forskjellen er store og små bokstaver, kan en av filene være utilgjengelig når du prøver å åpne det hemmelige hvelvet. For å unngå tap av data, anbefaler vi å legge til slike filer i forskjellige hemmelige hvelv eller endre filnavnene til helt unike navn.

Slik får du tilgang til filer som er lagret i et hemmelig hvelv

Slik får du tilgang til filer som er lagret i et hemmelig hvelv:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. I blokken **Hemmelig hvelv** klikker du på **Jeg har allerede et hemmelig hvelv**-knappen.

   Vinduet **Hemmelig hvelv** vil da åpne.
4. Klikk **Lås opp** ved siden av det hemmelige hvelvet.
5. Angi passordet, og klikk deretter på knappen **Åpne i Windows Utforsker**.

   Filene som er lagret i det hemmelige hvelvet, vises i Utforsker-vinduet. Du kan redigere filene ved behov, eller legge til nye filer og lukke det hemmelige hvelvet igjen.

Det kan oppstå en feil hvis du prøver å åpne et hemmelig hvelv som du har gitt nytt navn. For å unngå dette, anbefaler vi at du åpner det hemmelige hvelvet du vil døpe om og henter ut dataene, for så å opprette et nytt hemmelig hvelv med disse dataene og gi det et annet navn.

Noen ganger kan åpning av hemmelige hvelv opprettet i andre Kaspersky-programmer kreve konvertering av hemmelige hvelv fra det gamle formatet til det nye. Når du prøver å åpne et hemmelig hvelv i Kaspersky-programmets grensesnitt, vil Kaspersky-programmet foreslå konvertering om nødvendig.

Konvertering av et hemmelig hvelv til det nye formatet kan ta lang tid, avhengig av størrelsen på det hemmelige hvelvet.

Hvis avmerkingsboksen **Programmets driftsinnstillinger** er deaktivert i vinduet **Lagre følgende data på denne datamaskinen for senere bruk** når du fjerner programmet, og avmerkingsboksen **Hemmelig hvelv** er aktivert, må du legge til de hemmelige hvelvene manuelt ved å klikke på **Jeg har allerede et hemmelig hvelv** i vinduet **Hemmelig hvelv** neste gang du installerer den nåværende eller fremtidige versjonen av Kaspersky-programmet.

Filmakulering

Kun tilgjengelig i Kaspersky Plus og Kaspersky Premium.

En tilleggsfunksjon som hjelper til å sikre personlige data ved å beskytte slettet informasjon mot uautorisert gjenoppretting av hackere.

Kaspersky-programmet kommer med et verktøy for permanent sletting av data som gjør det umulig å gjenopprette data ved hjelp av standard gjenopprettingsverktøy.

Kaspersky-programmet gjør det mulig å slette data uten at de kan gjenopprettes fra følgende data medier:

- Lokale stasjoner. Sletting er mulig hvis brukeren har rettighetene som kreves for lagring og sletting av informasjon.
- Flyttbare stasjoner eller andre enheter som kan gjenkjennes som flyttbare stasjoner (f.eks. disketter, minnekort, USB-enheter eller mobiltelefoner). Data kan slettes fra et minnekort hvis den mekaniske beskyttelsen mot overskriving er deaktivert.

Du kan kun slette data som du har tilgang til via din personlige konto. Før du sletter data må du kontrollere at de ikke brukes av åpne programmer.

Slik sletter du data permanent:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. I blokken **Filmakulering** klikker du på **Velg filer**-knappen.

   Vinduet **Filmakulering** vil da åpne.
4. Klikk på **Bla gjennom**, og velg mappen eller filen som skal slettes permanent, i vinduet **Velg filer som skal slettes**.

   Sletting av systemfiler og -mapper kan føre til problemer i operativsystemet.
5. Fra rullegardinlisten **Metode for sletting av data** velger du dataslettingsalgoritmen du ønsker.

   Når du skal slette data fra SSD- og USB-enheter, anbefaler vi at du bruker metoden **Hurtig-slett (anbefales)** eller **GOST R 50739-95, Russland**. Andre slettingsmetoder kan skade SSD- eller USB-enheten.

   - **Hurtig-slett (anbefales)**. Sletteprosess som bruker to sykluser med overskriving av data: skriving av nuller og skriving av pseudovilkårlige tall. Hovedfordelen ved denne algoritmen er ytelsen. Hurtigsletting forhindrer at data kan gjenopprettes med standard gjenopprettingsverktøy.
   - **GOST R 50739-95, Russland**. Algoritmen utfører en overskrivingssyklus med pseudovilkårlige tall og beskytter dataene mot gjenoppretting med vanlige verktøy. Denne algoritmer tilsvarer beskyttelsesklasse 2 av 6, i henhold til klassifiseringen til den russiske State Technical Commission.
   - **Bruce Schneier-algoritme**. Prosessen består av sju overskrivingssykluser. Forskjellen i forhold til den tyske VSITR-metoden ligger i overskrivingssekvensen. Denne forbedrede metoden for sletting av data anses som den mest pålitelige.
   - **Standarden VSITR, Tyskland**. Sju overskrivingssykluser utføres. Algoritmen anses å være pålitelig, men kjøringen tar betraktelig lengre tid.
   - **Standarden NAVSO P-5239-26 (MFM), USA** og **Standarden NAVSO P-5239-26 (RLL), USA**. Det brukes tre overskrivingssykluser. Standardenes forskjeller ligger i sekvensene de bruker når de overskriver informasjonen.

- **Standarden DoD 5250.22-M, USA**. Algoritmen utfører tre overskrivingssykluser. Denne standarden brukes av det amerikanske forsvarsdepartementet.

6. Klikk på **Slett**.

7. Klikk på **Slett** i bekreftelsesvinduet som åpnes.

Filer som brukes av et tredjepartsprogram, kan ikke slettes.

Personvernrengjøring

Kun tilgjengelig i Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Brukerens handlinger på datamaskinen logges i operativsystemet. Følgende informasjon lagres:

- Detaljer om utførte søk og besøkte nettsteder
- Informasjon om programmer som er startet, og om filer som er åpnet og lagret
- Oppføringer i hendelsesloggene i Microsoft Windows
- Annen informasjon om brukeraktivitet

Inntrengere og uautoriserte personer vil kanskje kunne få tilgang til konfidensiell informasjon i informasjon fra tidligere brukerhandlinger.

Programmet kommer med en veiviser for personvernrengjøring, som rydder opp i spor etter brukeraktivitet i systemet.

Slik kjører du veiviseren for personvernrengjøring:

1. Åpne hovedvinduet.
2. Gå til delen **Personvern**.
3. I blokken **Personvernrengjøring** klikker du på **Finn aktivitet**-knappen.

Veiviseren består av en rekke skjermbilder (trinn) som du kan navigere i med knappene **Tilbake** og **Neste**. Klikk på **Fullført**-knappen for å lukke veiviseren når den er fullført. Du kan når som helst stoppe veiviseren ved å klikke på **Avbryt**.

La oss gå grundigere gjennom trinnene i veiviseren.

Starte Veiviseren

a. Velg ett av de to alternativene for veiviseroperasjonen:

- **Søk etter spor av brukeraktivitet**. Veiviseren starter et søk etter spor av dine aktiviteter på datamaskinen.
- **Rull tilbake endringer**. Veiviseren vil rulle tilbake endringene som tidligere ble gjort av veiviseren for personvernrengjøring. Dette alternativet er tilgjengelig hvis veiviseren har fjernet aktivitetsspor før.

b. Klikk på **Neste** for å starte veiviseren.

Søk etter aktivitetsspor

Hvis du valgte alternativet **Søk etter spor av brukeraktivitet**, utfører veiviseren et søk etter spor av aktivitet på datamaskinen. Søket kan ta litt tid. Når søket er fullført, fortsetter veiviseren automatisk videre til neste trinn.

Velge handlinger for Personvernrengjøring

Når søket er fullført, informerer veiviseren deg om aktivitetssporene og spør om handlingene som skal utføres for å eliminere disse aktivitetssporene.

Hvis du vil vise handlinger som er inkludert i en gruppe, kan du utvide listen for den valgte gruppen.

Hvis du vil at veiviseren skal utføre en viss handling, må du merke av i den tilhørende boksen ved siden av handlingen. Som standard utfører veiviseren alle anbefalte og sterkt anbefalte handlinger. Hvis du ikke ønsker å utføre en bestemt handling, fjerner du avmerkingen i boksen ved siden av handlingen.

Vi anbefaler på det sterkeste at du ikke deaktiverer bokser som er aktivert som standard, fordi det vil føre til at datamaskinen blir sårbar for trusler.

Etter at du har definert settet med handlinger som veiviseren skal utføre, klikker du på **Neste**.

Personvernrengjøring

Veiviseren vil utføre handlingene som ble valgt på det forrige trinnet. Det kan ta litt tid å rydde opp aktivitetsspor. Hvis du vil rydde opp i aktivitetsspor, må du eventuelt starte datamaskinen på nytt. Hvis det er tilfellet, vil veiviseren varsle deg om det.

Når oppryddingen er fullført, vil veiviseren automatisk gå videre til neste trinn.

Fullføring av veiviseren

Klikk på **Fullført** for å avslutte veiviseren.

Beskytte personlige data på Internett

I denne delen finner du informasjon om hvordan du konfigurerer trygg surfing på Internett og beskytter dataene dine mot tyveri.

Om beskyttelse av personlige data på Internett

Kaspersky-programmet beskytter de personlige dataene dine mot tyveri:

- Passord, brukernavn og andre registreringsdata
- Kontonumre og bankkortnumre

Kaspersky-programmet inkluderer komponenter og verktøy som hjelper til å beskytte dine personlige data mot tyveriforsøk av kriminelle. De bruker metoder som for eksempel phishing og oppfanging av data som tastes inn på tastaturet.

Beskyttelse mot nettfisking tilbys av funksjonen Anti-Phishing, som er innebygd i komponentene Sikker surfing og Anti-Spam. Aktiver disse komponentene for å sikre avansert beskyttelse mot phishing.

Skjermtastatur og Sikkert tastaturinntasting gir beskyttelse mot oppfanging av data som tastes inn på datamaskintastaturet.

Veiviseren for personvernrengjøring sletter all informasjon om brukerens aktiviteter på datamaskinen.

Safe Money og Kaspersky VPN beskytter data når du bruker nettbanktjenester og nettbutikker.

Om Skjermtastatur

Når du surfer på nettet, må du ofte oppgi personlige data eller brukernavn og passord. Det kan for eksempel være nødvendig når du registrerer deg for kontoer på nettsteder eller bruker netthandel eller nettbank.

Det er fare for at disse personlige dataene blir fanget opp ved bruk av keyloggere, det vil si programmer som registrerer tastetrykk. Verktøyet Skjermtastatur forhindrer oppfanging av data via tastaturet.

Mange programmer som er klassifisert som spionprogrammer, kan ta skjermbilder og automatisk sende disse til en inntrenger, som vil analysere dem og stjele brukerens personlige data. Skjermtastatur beskytter personlige data som skrives inn, mot oppfangingsforsøk ved hjelp av skjermbilder.

Skjermtastatur har følgende funksjoner:

- Du kan klikke på tastene til skjermtastaturet med musen.
- Du kan ikke klikke på flere taster samtidig på et skjermtastatur, i motsetning til på datamaskintastaturer. Hvis du vil bruke tastekombinasjoner (for eksempel **ALT**+**F4**), må du derfor først trykke på den første tasten (for eksempel **ALT**), så trykke på den andre tasten (for eksempel **F4**), og deretter trykke på den første tasten på nytt. Andre klikk på samme tast har samme virkning som å slippe opp tasten på et datamaskintastatur.
- Du kan bytte språk på skjermtastaturet ved å bruke de samme snarveiene som er konfigurert for datamaskintastaturet i innstillingene til operativsystemet. Du må høyreklikke på den andre tasten (hvis for eksempel snarveien **VENSTRE ALT**+**SHIFT** er konfigurert for å bytte tastaturspråk i operativsystemet, må du venstreklikke på tasten **VENSTRE ALT** og deretter høyreklikke på **SHIFT**-tasten).

Du må starte datamaskinen på nytt etter at du har installert Kaspersky-programmet, for å garantere at data som angis via Skjermtastatur, er beskyttet.

Bruk av Skjermtastatur har følgende begrensninger:

- Skjermtastatur forhindrer kun oppfanging av personlige data når du bruker Chromium-baserte nettlesere som Microsoft Edge, Mozilla Firefox eller Google Chrome. Hvis du bruker Skjermtastatur med andre nettlesere, beskyttes ikke personlige data mot oppfanging.
- Skjermtastatur kan ikke beskytte dine personlige data hvis nettstedet som krever registrering av slike data, er hacket, fordi informasjonen da hentes inn direkte av inntrengere.
- Skjermtastatur forhindrer ikke skjermdumper som aktiveres med tasten **Print Screen** og andre tastekombinasjoner som er angitt i innstillingene til operativsystemet, eller ved hjelp av DirectX.
- Kaspersky-programmet beskytter ikke mot uautoriserte skjermdumper i Microsoft Windows 8 og 8.1 (kun 64-biters) hvis vinduet Skjermtastatur er åpent, men Beskyttet nettleser ikke er startet.

Slik åpner du skjermtastaturet

Du kan åpne Skjermtastatur på følgende måter:

- Fra verktøylinjen i Chromium-basert Microsoft Edge, Mozilla Firefox eller Google Chrome

- Ved å bruke hurtigstartikonet for Skjermtastatur i registreringsfeltene på nettsteder

  Du kan konfigurere visning av hurtigstartikonet i registreringsfeltene på nettsteder.

  Når du bruker Skjermtastatur, vil Kaspersky-programmet deaktivere alternativet for automatisk utfylling av registreringsfelter på nettsteder.

- Ved å bruke en tastekombinasjon

Starte skjermtastaturet fra nettleserens verktøylinje

Slik åpner du Skjermtastatur fra verktøylinjen i nettlesere som Microsoft Edge basert på Chromium, Mozilla Firefox eller Google Chrome:

1. Klikk på knappen **Kaspersky Protection** på verktøylinjen i nettleseren.
2. Velg elementet **Skjermtastatur** på menyen som åpnes.

Starte skjermtastaturet ved bruk av datamaskintastaturet

Slik åpner du Skjermtastatur ved hjelp av datamaskintastaturet:

Bruker du tastekombinasjonen **CTRL+ALT+SHIFT+P**.

Denne snarveien viser ikke skjermtastaturet hvis snarveien allerede er i bruk av et annet program, for eksempel Microsoft Word.

Slik konfigurerer du visning av ikonet for Skjermtastatur

Slik konfigurerer du visning av hurtigstartikonet for Skjermtastatur i registreringsfeltene på nettsteder:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Personverninnstillinger**.
4. I vinduet **Personverninnstillinger** klikker du på **Sikkert datainput**-knappen.
   Vinduet viser innstillinger for beskyttelse av datainntasting.
5. I delen **Skjermtastatur** merker du av for alternativet **Åpne Virtuelt tastatur med tastekombinasjonen CTRL+ALT+SHIFT+P**.
6. Hvis du vil at hurtigstartikonet for Skjermtastatur skal vises i registreringsfeltene på alle nettsteder, merker du av for alternativet **Vis ikonet for hurtigoppstart i dataregistreringsfelter**.

7. Hvis du ønsker at hurtigstartikonet for skjermtastaturet bare skal vises når du åpner spesifikke nettstedkategorier, krysser du av i avmerkingsboksene for nettstedkategoriene der du vil at ikonet skal vises i inntastingsfeltene.

   Hurtigstartikonet for Skjermtastatur vises når du åpner et nettsted som tilhører en av de valgte kategoriene.

8. Slik aktiverer og deaktiverer du visning av hurtigstartikonet for Skjermtastatur på et bestemt nettsted:

   a. I seksjonen **Skjermtastatur** klikker du på lenken **Behandle unntak** for å åpne vinduet **Unntak for skjermtastatur**.

   b. Klikk på **Legg til** nederst i vinduet.

   c. Et vindu der du kan legge til et unntak for Skjermtastatur, åpnes.

   d. Angi nettadressen til et nettsted i feltet **Nettadressemaske**.

   e. I delen **Omfang** angir du om du vil at hurtigstartikonet for Skjermtastatur skal vises: på den angitte siden eller på alle sidene til nettstedet.

   f. I delen **Ikon for skjermtastatur** angir du om du vil at hurtigstartikonet for Skjermtastatur skal vises.

   g. Klikk på **OK**.

      Det angitte nettstedet vises på listen i vinduet **Unntak for skjermtastatur**.

Når du åpner det angitte nettstedet, vises hurtigstartikonet for Skjermtastatur i registreringsfeltene i henhold til de angitte innstillingene.

Om beskyttelse av data angitt på datamaskintastaturet

Ved å beskytte inntasting av data på datamaskintastaturet kan du forhindre at disse dataene du taster inn på nettsteder blir fanget opp av uvedkommende. Utvidelsen for Kaspersky Protection må være aktivert for å beskytte datainntasting på tastaturet. Du kan konfigurerer beskyttelse av dataregistrering fra datamaskintastaturet på ulike nettsteder. Etter at Sikkert tastaturinput er aktivert, vil en popup-melding om at Sikkert tastaturinput er aktivert vises ved siden av feltet der markøren er plassert. Sikkert tastaturinput er aktivert som standard for alle nettstedkategorier, med unntak av Internettkommunikasjon.

Innstillinger for Sikkert tastaturinput

Sikkert datainput i Kaspersky-programmet har følgende begrensninger:

- Sikkert tastaturinput fungerer ikke i nettlesere som kjører i programmet Sandboxie.
- Sikkert tastaturinput kan ikke beskytte de personlige dataene dine hvis nettstedet der du legger inn slike data, er hacket, ettersom informasjonen da blir omdirigert direkte til inntrengerne. Sikkert tastaturinput fungerer bare i følgende nettlesere: Microsoft Edge basert på Chromium, Mozilla Firefox, Mozilla Firefox ESR og Google Chrome når Kaspersky Protection-utvidelsen er installert og aktivert.
- Beskyttelse fungerer kun på sider som oppfyller følgende betingelser:
  - Siden er i en liste over URL-adresser eller en sidekategori som krever Sikkert tastaturinput.
  - Siden er åpen i en beskyttet nettleser.

- Siden er ikke på unntakslisten for URL-adresser.
- Siden inneholder et felt for angivelse av passord. Samtidig bør alternativet **Felt for angivelse av passord på alle nettsteder** være valgt i programinnstillingene.
- Bekreft om avmerkingsboksen er merket av ved å gå til delen **Personverninnstillinger** → **Sikkert datainput** → blokken **Sikkert tastaturinput**.

- Beskyttelse fungerer kun på felter som oppfyller følgende betingelser:
  - Inntastingsfeltet er ´én linje, og det tilsvarer med <input>-taggen for HTML.
  - Inntastingsfeltet er ikke skjult: Verdien til typeattributtet er ikke «lik» skjult, og i CSS-stiler er visningsfeltet ikke satt til «ingen».
  - Inntastingsfeltet er ikke felter av typene for innsending, radio, avmerkingsbokser, knapper eller bildetyper.
  - Inntastingsfeltet kan ikke være skrivebeskyttet (readOnly).
  - Inntastingsfeltet må være klart for inntasting (get focus).
  - Hvis feltet har attributtet for maksimal lengde (maxlength), bør minste antall tegn som kan tastes inn være mer enn tre.
- Beskyttelse fungerer ikke i følgende tilfeller:
  - Data legges inn ved hjelp av IME-teknologien.
  - Inntastingsfeltet er ikke et felt for inntasting av passord.

I perioden etter at du har installert Kaspersky-programmet, men før du starter datamaskinen på nytt for første gang, vil programmet ikke få med seg det første tegnet brukeren skriver inn (i noe program).

Hvis du har problemer, kan du sende en forespørsel med en detaljert beskrivelse av problemet til teamet hos Kasperskys tekniske støtte via My Kaspersky.

Se Hjelp for instruksjoner om hvordan du arbeider med My Kaspersky.

Slik konfigurerer du beskyttelse av data angitt på datamaskintastaturet

Slik konfigurerer du beskyttelse av data angitt på datamaskintastaturet:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Gå til delen **Personverninnstillinger**.
4. Klikk på **Sikkert datainput**.

   Vinduet **Innstillinger for Sikkert datainput** vil da åpne.
5. Gå til delen **Sikkert tastaturinput** i nedre del av vinduet, og merk av for alternativet **Aktiver sikkert tastaturinput**.

6. Merk av i boksene for kategoriene med nettsteder der du vil beskytte inntasting av data via tastaturet.

7. Slik aktiverer eller deaktiverer du beskyttelse av dataregistrering fra tastaturet for et bestemt nettsted:

   a. Åpne vinduet **Unntak for skjermtastatur** ved å klikke på koblingen **Behandle unntak**.

   b. Klikk på **Legg til** i vinduet som åpnes.

   c. Et vindu der du kan legge til et unntak for Sikkert tastaturinput, åpnes.

   d. I vinduet som åpnes, angir du en nettadresse i feltet **Nettadressemaske**.

   e. Velg ett av alternativene for Sikkert datainput på dette nettstedet (**Bruk på angitt side** eller **Bruk på hele nettstedet**).

   f. Velg handlingen som skal utføres av Sikkert datainput på dette nettstedet (**Beskytt** eller **Ikke beskytt**).

   g. Klikk på **OK**.

Det angitte nettstedet vises på listen i vinduet **Unntak for skjermtastatur**. Når du åpner dette nettstedet, vil Sikkert datainput være aktivt og kjøre i henhold til innstillingene.

Kontrollere sikkerheten til et nettsted

Med Kaspersky-programmet kan du sjekke om et nettsted er trygt før du klikker på en kobling for å åpne det. Nettsteder kontrolleres ved hjelp av *URL-veileder*.

Komponenten URL-veileder kontrollerer lenken på nettsider som åpnes i Chromium-basert Microsoft Edge, Google Chrome og Mozilla Firefox. Kaspersky-programmet viser ett av følgende ikoner ved siden av hver kobling som er kontrollert:

– hvis det lenkede nettstedet er sikkert ifølge Kaspersky

– hvis det ikke finnes informasjon om sikkerhetsstatusen til den koblede websiden

– hvis Kaspersky mener at hackere kan forårsake skade på datamaskinen din eller dataene dine hvis du bruker nettsiden som koblingen åpner

– vis Kaspersky mener at nettsiden som koblingen åpner kan være infisert eller hacket

– hvis det lenkede nettstedet er farlig ifølge Kaspersky
Hvis du vil vise et popup-vindu med mer informasjon om koblingen, peker du på det tilhørende ikonet.

Kaspersky-programmet kontrollerer som standard kun koblinger i søkeresultater. Du kan aktivere kontroll av URL-adresser på hvert nettsted.

Slik konfigurerer du kontroll av URL-adresser på nettsteder:

1. Åpne hovedvinduet.

2. Klikk på -knappen nederst i hovedvinduet.
   Vinduet **Innstillinger** vil da åpne.

3. Velg delen **Sikkerhetsinnstillinger**.

4. Klikk på **Sikker surfing**.

   Vinduet **Innstillinger for Sikker surfing** vil da åpne.

5. Klikk på koblingen **Avanserte innstillinger** for å åpne avanserte innstillinger for Sikker surfing.

6. I blokken **URL-veileder** velger du alternativet **Kontroller URLer**.

7. Hvis du vil at Kaspersky-programmet skal skanne innholdet på alle nettsteder, merker du av for alternativet **På alle nettsteder unntatt de som er angitt**.

8. Om nødvendig kan du angi websider du stoler på (klarerer), i vinduet **Unntak**. Åpne dette vinduet ved å klikke på koblingen **Behandle unntak**. Kaspersky-programmet vil ikke skanne innholdet på de spesifiserte websidene.

9. Hvis du vil at Kaspersky-programmet kun skal sjekke innholdet på bestemte websider:

   a. Velg alternativet **Kun på angitte nettsteder**.

   b. Klikk på **Konfigurer kontrollerte nettsteder** for å åpne vinduet **Kontrollerte nettsteder**.

   c. Klikk på **Legg til**.

   d. Skriv inn adressen til websiden du vil kontrollere innholdet på.

   e. Velg status for kontroll av websider (hvis statusen er *Aktiv*, kontrollerer Kaspersky-programmet innholdet på websider).

   f. Klikk på **OK**.

      Den angitte nettsiden vises på listen i vinduet **Kontrollerte nettsteder**. Kaspersky-programmet sjekker URL-adresser på denne websiden.

10. Hvis du vil redigere avanserte innstillinger for kontroll av URL-adresser, går du til vinduet **Avanserte innstillinger for Sikker surfing**. Deretter går du til delen **URL-veileder** og klikker på koblingen **Konfigurer URL-veileder** for å åpne vinduet **Kontrollerte URLer**.

11. Hvis du vil at Kaspersky-programmet skal varsle deg om sikkerheten til koblingene på alle websider, går du til delen **Kontrollerte URLer** og velger **Alle URLer**.

12. Hvis du vil at Kaspersky-programmet skal vise informasjon som angir om en kobling tilhører en bestemt kategori med nettsteder (for eksempel *banning, uanstendighet*):

    a. Aktiver avmerkingsboksen **Upassende eller grovt språk**.

    b. Aktiver avmerkingsboksene ved siden av kategoriene med nettstedinnhold som du vil se informasjon om i kommentarene.

Kaspersky-programmet kontrollerer koblingene på bestemte websider og viser informasjon om kategoriene med koblinger i henhold til de valgte innstillingene.

Slik endrer du innstillinger for krypterte tilkoblinger

Krypterte tilkoblinger etableres over SSL- og TLS-protokoller. Som standard skanner Kaspersky-programmet slike tilkoblinger på forespørsel fra beskyttelseskomponenter, for eksempel E-post-Antivirus, Anti-Spam, Safe Money, URL-veileder, Privat surfing, Sikker surfing og Anti-Banner.

Slik endrer du innstillinger for krypterte tilkoblinger:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Gå til delen **Sikkerhetsinnstillinger**.
4. I blokken **Avanserte innstillinger** klikker du på **Nettverksinnstillinger**-knappen.
5. I vinduet **Nettverksinnstillinger** går du til delen **Skanning av krypterte tilkoblinger**.
6. Velg en handling som skal utføres ved tilkobling til nettsteder over kryptert tilkobling:

   - **Ikke skann krypterte tilkoblinger**. Programmet skanner ikke krypterte tilkoblinger.
   - **Skann krypterte tilkoblinger på forespørsel fra beskyttelseskomponenter**. Kaspersky-programmet skanner kun krypterte tilkoblinger på forespørsel fra URL-veileder. Denne handlingen er valgt som standard.
   - **Skann alltid krypterte tilkoblinger**. Kaspersky-programmet skanner alltid krypterte tilkoblinger.

   Hvis du klikker på **Vis sertifikater**, åpnes et vindu med en liste over klarerte sertifikater som brukes av populære nettsteder. Sertifikater legges til på denne listen hvis du klikker på **Legg til som klarert sertifikat og fortsett** i en Kaspersky-advarsel når du besøker et nettsted. Etter at du har lagt til et sertifikat i listen, anses nettstedet som klarert. Du kan legge til eller fjerne sertifikater i vinduet **Klarerte rotsertifikater** ved hjelp av knappene **Legg til** og **Slett**.

   Hvis du har flere brukerkontoer på datamaskinen, og en av brukerne godtar det nye sertifikatet, legges dette sertifikatet også til på listen over klarerte sertifikater for alle andre brukere.
7. Velg en handling som skal utføres hvis det oppstår feil ved skanning av krypterte tilkoblinger:

   - **Ignorer**. Hvis denne handlingen er valgt, avslutter Kaspersky-programmet tilkoblingen med nettstedet hvor skannefeilen oppstod.
   - **Spør**. Hvis det oppstår en feil ved skanning av krypterte tilkoblinger med et nettsted, viser Kaspersky-programmet en varsling hvor du kan velge en handling:

     - **Ignorer**. Kaspersky-programmet avslutter tilkoblingen med nettstedet hvor skannefeilen oppstod.
     - **Legg til domenet i unntak**. Kaspersky-programmet legger til nettadressen i listen over klarerte adresser. Kaspersky-programmet skanner ikke krypterte tilkoblinger på nettsteder oppført i listen over klarerte adresser. Du kan se slike nettsteder ved å klikke på **Klarerte adresser**.

     Dette alternativet er valgt som standard.
   - **Legg til domenet i unntak**. Kaspersky-programmet legger nettstedet til i listen over klarerte adresser. Kaspersky-programmet skanner ikke krypterte tilkoblinger på nettsteder oppført i listen over klarerte adresser. Disse nettstedene er vist i vinduet **Klarerte adresser**, som kan åpnes ved å klikke på lenken **Klarerte adresser**.
8. Klikk **Klarerte adresser** for å åpne vinduet **Klarerte adresser** og utføre følgende handlinger:

a. Klikk **Legg til**-knappen for å legge til nettstedet i listen over unntak for skanning av krypterte tilkoblinger.

b. Angi domenenavnet til nettstedet i feltet **Domenenavn**.

c. Klikk på **Legg til**.

Kaspersky-programmet skanner ikke krypterte tilkoblinger med dette nettstedet. Vær oppmerksom på at det å legge til et nettsted i listen over klarerte adresser kan begrense funksjonaliteten for skanning av nettstedet for beskyttelseskomponenter, for eksempel Safe Money, URL-veileder, Privat surfing, Sikker surfing og Anti-Banner.

Om sikker tilkobling til trådløse nettverk

Kun tilgjengelig i Kaspersky Plus og Kaspersky Premium.

Offentlige trådløse nettverk kan være underbeskyttede, for eksempel hvis et trådløst nettverk bruker en sårbar krypteringsprotokoll eller et svakt passord. Når du gjennomfører nettkjøp over usikre trådløse nettverk, sendes passordene dine og andre konfidensielle data som ikke kryptert tekst. Hackere kan fange opp de konfidensielle dataene dine, f.eks. bankkortnummeret ditt, og få tilgang til pengene dine.

For å sikre sikkerheten din når du bruker usikre trådløse nettverk, kan du aktivere VPN via en spesielt tilordnet server plassert i regionen du spesifiserer. Trafikk fra nettstedet går først til den tilordnede serveren, før den sendes til enheten via en kryptert sikker tilkobling.

Du må kjøre Kaspersky VPN for å bruke Kaspersky VPN-komponenten. Kaspersky VPN Secure Connection installeres sammen med Kaspersky-programmet på Kaspersky Plus-planen.

Komponenten Kaspersky VPN gir følgende fordeler:

- Sikker bruk av betalingssystemer og nettsteder for bestilling. Inntrengere vil ikke kunne fange opp bankkortnumrene dine når du betaler på nett, bestiller hotellrom eller leier biler.
- Beskyttelse av konfidensiell informasjon. Ingen vil kunne finne datamaskinens IP-adresse eller plassering.
- Beskyttelse av personvernet ditt. Ingen vil kunne fange opp og lese private samtaler du har på sosiale nettverk.

VPN-tilkobling kan også brukes til andre typer nettverksforbindelser, for eksempel en lokal internettforbindelse eller tilkobling via et USB-modem.

Kaspersky VPN Secure Connection vil som standard ikke aktivere en VPN-tilkobling hvis HTTPS-protokollen brukes til å koble til et nettsted.

Endring av region eller by ved besøk på nettstedene til nettbanker, betalingssystemer, nettsteder for bestilling, sosiale nettverk, chatter og e-postklienter kan utløse systemer mot svindel (systemer beregnet på å analysere finansielle transaksjoner for å finne tegn på bedrageri).

Bruk av VPN-tilkobling kan være regulert av lokal lovgivning. Du tillates kun å bruke VPN-tilkobling i henhold til programmets formål, og uten å bryte lokale lover og bestemmelser.

Konfigurere varsling om sårbarheter i trådløse nettverk

Hvis Kaspersky VPN Secure Connection ikke er installert på datamaskinen, viser Kaspersky-programmet et varsel om tilkobling til trådløse nettverk og usikker overføring av passordet over Internett. Du kan tillate eller blokkere tilkobling og overføring av passord fra varslingsvinduet.

Etter at du har installert Kaspersky VPN Secure Connection, deaktiveres innstillingene for visning av varsler når du kobler til trådløse nettverk og overfører et ikke-kryptert passord. Du kan konfigurere varslingsinnstillingene for trådløse nettverksforbindelser i Kaspersky VPN Secure Connection.

Slik konfigurerer du varsling om sårbarheter i trådløse nettverk:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. Velg delen **Sikkerhetsinnstillinger**.
4. Aktiver komponenten **Brannmur**.

   Vinduet viser innstillingene for komponenten Brannmur.
5. Velg **Varsle om sårbarheter i trådløse nettverk** hvis du vil motta varslinger når du kobler til sårbare trådløse nettverk. Hvis du ikke vil motta varslinger, deaktiverer du alternativet. Dette alternativet kan velges hvis Kaspersky VPN Secure Connection ikke er installert på datamaskinen.
6. Klikk på **Velg kategorier** og velg sårbarhetskategorier for trådløse nettverk. Kaspersky-programmet vil varsle deg når du prøver å koble til et trådløst nettverk med den relevante sårbarheten.
7. Hvis alternativet **Varsle om sårbarheter i trådløse nettverk** er aktivert, kan du redigere avanserte innstillinger for visning av varslinger:

   - Merk av for **Blokker og advar om usikker overføring av passord over Internett** hvis du vil blokkere enhver overføring av passord som ikke-kryptert tekst når du fyller inn **Passord**-felter på Internett.
   - Klikk på lenken **Aktiver** for å gjenopprette standardinnstillingene for visning av varslinger om overføring av passord som ikke er kryptert. Hvis du har blokkert visning av varslinger om overføring av passord som ikke er kryptert, vil varslingene vises igjen.

Når du kobler til beskyttede trådløse nettverk, viser programmet et varsel som spør deg om du stoler på det nye nettverket. Du kan velge ett av følgende alternativer:

- **Nei, blokker ekstern tilgang til datamaskinen**. Alle eksterne tilkoblinger til dette nettverket er blokkert, bortsett fra tilkoblinger som startes fra enheten din. Du kan bruke Internett og besøke alle nettsteder. Andre brukere på dette nettverket vil ikke kunne koble til ressursene på datamaskinen din (de vil for eksempel ikke ha tilgang til innholdet på diskene dine, inkludert i delte mapper).
- **Begrens, men tillat delt tilgang**. Du kan bruke Internett og besøke alle nettsteder. Andre brukere på dette nettverket vil ikke ha tilgang til ressursene på datamaskinen din, men de vil ha tilgang til ressurser som er utpekt som delte (for eksempel delte mapper).
- **Ja, tillat all nettverksaktivitet**. Alle tilkoblinger på dette nettverket tillates. Du kan bruke Internett og besøke alle nettsteder. Andre brukere på dette nettverket vil kunne koble til datamaskinen din, uten begrensninger (de vil for eksempel kunne få tilgang til innholdet på diskene dine).

Identitet

Kaspersky Premium inkluderer verktøy for å beskytte den digitale identiteten din, og en egen kanal for å kontakte teknisk støtte.

Lommebok for identitetsbeskyttelse

Hvis du oppbevarer viktige dokumenter på datamaskinen, for eksempel skanninger av legitimasjon, offentlige dokumenter, kontrakter og så videre, anbefaler vi å legge slike dokumenter i den sikre lommeboken. Lommebok for identitetsbeskyttelse er en kryptert fil som krever hovedpassord for å gå tilgang. Dette garanterer sikkerheten til de personlige dataene dine ved å hindre at tredjeparter får tilgang til dokumentene.

Om hovedpassordet

Hovedpassordet er ett passord som Kaspersky-programmet bruker til å kryptere dataene dine i lommeboken. Vi anbefaler å bruke et hovedpassord med åtte eller flere tegn, med store og små bokstaver, tall og spesialtegn.

Av sikkerhetsgrunner lagrer ikke Kaspersky-programmet hovedpassordet på enhetene dine, og sender det ikke til skylageret. Vi anbefaler å huske hovedpassordet eller å skrive det ned og oppbevare det på et sikkert sted, fordi det ikke er mulig å gjenopprette et glemt passord.

Om kryptering

Kaspersky-programmet krypterer data med en symmetrisk krypteringsalgoritme basert på standarden Advanced Encryption Standard (AES). Nøkkelen beregnes fra hovedpassordet ditt basert på Password-Based Key Derivation Function 2 (PBKDF2). AES-algoritmen er mye brukt over hele verden til å beskytte hemmelige data. Denne algoritmen krever minimalt med RAM, slik at dataene dine kan krypteres og dekrypteres i løpet av sekunder.

Slik legger du til et dokument i lommeboken

1. Åpne hovedvinduet.
2. Gå til delen **Identitet**.
3. Under **Lommebok for identitetsbeskyttelse**:
   - Hvis lommeboken ikke er tilkoblet enda, klikker du på **Last ned** for å laste ned Kaspersky Password Manager-programmet, hvis det ikke er installert enda. Knappen kan hete **Start** eller **Åpne** hvis Kaspersky Password Manager ikke er konfigurert, er utdatert eller er koblet til en My Kaspersky-konto som ikke stemmer overens med kontoen som Kaspersky-programmet er koblet til.
     a. Følg instruksjonene i installasjonsveiviseren for å laste ned og installere Kaspersky Password Manager.
     b. Kaspersky-programmet foreslår å opprette og koble til en lommebok. Følg instruksjonene i veiviseren. Når du kobler til en lommebok, blir du også bedt om å opprette et hovedpassord.
   - Hvis du allerede har koblet til en lommebok, klikker du på **Legg til dokument**.
     1. Under **Dokumenter** klikker du på **Legg til dokument**.
     2. I rullegardinmenyen velger du:
        - **Bla etter filer**. Utforskervinduet åpnes. I feltet **Filnavn** angir du banen til filen og klikker på **Åpne**. Velg en kategori for dokumentet (for raskt søk i fremtiden) og klikk på **Legg til**.
        - **Søk automatisk**. Programmet søker etter JPEG-, PNG-, BMP- og PDF-filer som inneholder tekst. Filer som blir funnet, analysert og kategorisert som offentlig utstedt legitimasjon eller bankkort. Velg dokumentene og klikk på **Ferdig**.

De valgte dokumentene legges til i lommeboken som JPEG- eller PDF-filer.

Slik henter du ut et dokument fra lommeboken

1. Åpne hovedvinduet.
2. Gå til delen **Identitet**.
3. Under **Lommebok for identitetsbeskyttelse** klikker du på **Legg til dokument**.
4. Skriv inn hovedpassordet.
5. Velg ett dokument, eller hold inne Shift og klikk for å velge flere dokumenter.
6. Last ned dokumenter på en av følgende måter:
   - Høyreklikk for å åpne hurtigmenyen til dokumentet, og velg **Last ned**.
   - Klikk på ⋮ og velg **Last ned** i menyen som vises.
7. I vinduet **Lagre i mappe** angir du hvor du vil lagre dokumentet.
8. Om nødvendig kan du redigere navnet til dokumentet.
9. Klikk på **Lagre**.

   Dokumentet er lagret på enheten din. Formatet til nedlastede filer er det samme som formatet til de tilsvarende dokumentene i lommeboken (JPEG eller PDF).

Deteksjon av fjerntilgang

Fjerntilgangsprogrammer er legitim programvare for å koble til en ekstern datamaskin over nettverket. Fjerntilgangsprogrammer inkluderer TeamViewer, LogMeIn Pro og Remotely Anywhere. Hackere kan bruke slike programmer for å få kontroll over datamaskinen din, installere skadelig programvare, utgi seg for å være deg eller begynne å spionere på deg.

Vi sjekker om fjerntilgangsprogrammer er installert på datamaskinen din, og hjelper deg med å fjerne slike programmer for å hindre at noen får kontroll over enheten din.

Slik finner du fjerntilgangsprogrammer på datamaskinen din:

1. Åpne hovedvinduet.
2. Gå til delen **Identitet**.
3. I blokken **Deteksjon av fjerntilgang** klikker du på **Vis**.
4. Dette åpner vinduet **Deteksjon av fjerntilgang**. I dette vinduet kan du se hvilke fjerntilgangsprogrammer som ble funnet på datamaskinen din.

   Her er hva du kan gjøre i dette vinduet:

   - Klikk på **Detaljer** ved siden av et fjerntilgangsprogram for å se en kort beskrivelse av programmet.
   - Velg **Fjern** i rullegardinlisten ved siden av et program for å fjerne det. Dette tar deg til vinduet **Programmer og funksjoner**, der du kan fjerne det aktuelle programmet.

- Velg **Overse** i rullegardinlisten ved siden av et program hvis du ikke vil fjerne programmet akkurat nå. Programmet legges til i gruppen **Skjult**, og du vil kunne gå tilbake til det senere.

Søk etter fjerntilgangsprogrammer fungerer ikke hvis komponenten Inntrengningsbeskyttelse er deaktivert.

Premium-støttetjenester

Kasperskys Premium-støttetjenester over telefon er ikke tilgjengelig i enkelte områder. Du må ha et betalt abonnement for å kunne bruke Premium-støttetjenester.

Med Premium-støtte får du ekstra beskyttelse og bekvemmelighet, inkludert prioritert tilgang, ekspertinstallasjonstjenester, virussjekk og fjerning og PC-helsesjekk.

Installasjonstjenester fra eksperter

Du kan ringe oss hvis du har et installasjonsproblem på datamaskinen, så vil Kaspersky-eksperten hjelpe deg med følgende eksternt:

- kjøre installasjonen via fjerntilkobling
- sørge for at installasjonsprosessen er feilfri
- gi en oversikt over innstillinger og funksjoner i programmet
- svare på alle spørsmålene dine om programmet og installasjonsprosessen
- tilpasse programinnstillingene basert på behovene dine
- Bekrefte at programmet er installert, satt opp riktig og fungerer som det skal

Prioritert støttelinje

Prioritert tilgang til premium-støtte via telefon eller chat Kundetelefonsamtaler gis høyeste prioritet (først i køen). Chatteprogrammet inkluderer funksjoner for fjernhjelp.

Eksterne IT-tjenester

Tilgang med ett klikk for å snakke med en Premium-støtteagent, med ubegrenset fjernhjelp. Len deg tilbake og slapp av mens vi tar oss av problemet!

Søk etter og fjerning av virus fra eksperter

Profesjonell fjerning av virus og spionprogramvare på Windows-enheter med et Kaspersky-program installert

Tjenester for PC-helsesjekk

Under en helsesjekk vil ekspertene våre kjøre en kontroll av flere punkter for å sikre at enheten har best mulig beskyttelse og ytelse.

Hvis du vil bruke Kasperskys Premium-støttetjenester, ringer du telefonnummeret for landet du kjøpte Kaspersky Premium-abonnementet i.

Slik avinstallerer du inkompatible programmer

Kaspersky-programmet sjekker regelmessig om det finnes inkompatible programmer på datamaskinen. Slike programmer legges til i listen over inkompatible programmer. Du kan se gjennom listen og bestemme deg for hva du vil gjøre med de inkompatible programmene.

Det anbefales at du sletter inkompatible programmer fra datamaskinen. Ellers vil ikke Kaspersky-programmet kunne beskytte datamaskinen din.

Her er noen av årsakene til at et tredjepartsprogram kanskje ikke er kompatibelt med Kaspersky-programmet:

- Programmet er i konflikt med Fil-Antivirus.
- Programmet er i konflikt med brannmuren.
- Programmet er i konflikt med Anti-Spam.
- Programmet forstyrrer beskyttelse av nettverkstrafikk.
- Programmet er i konflikt med Hemmelig hvelv.
- Programmet er i konflikt med Kaspersky Password Manager.

Slik avinstallerer du inkompatible programmer

Slik fjerner du ukompatible programmer:

1. Åpne hovedvinduet.
2. Klikk på **Detaljer**-knappen øverst i vinduet.

   Vinduet **Varslingssenter** vil da åpne.
3. I delen **Anbefalinger** klikker du på **Vis** i linjen som inneholder meldingen om at det er oppdaget inkompatible programmer.

   Dette åpner vinduet **Fant inkompatibel programvare** med en liste over inkompatible programmer som ble oppdaget.
4. Aktiver alternativene ved siden av navnene på inkompatible programmer du ønsker å fjerne, og klikk på **Fjern**. Fjerningen gjøres av fjerningsverktøyene til disse programmene. I løpet av fjerningsprosessen kan det være at du blir bedt om å gi ditt samtykke til å fjerne eller endre innstillingene i tilknytning til fjerning av programmet.
5. Hvis datamaskinen fortsatt inneholder inkompatible programmer som ikke kan fjerne automatisk, åpnes et vindu som viser en liste over slike programmer. For å fjerne inkompatible programmer manuelt, klikker du på **Fjern manuelt**. Dette åpner et standard operativsystemvindu med en liste over installerte programmer. Fjern inkompatible programmer i henhold til instruksjonene for ditt operativsystem.
6. Start datamaskinen på nytt etter at du har fjernet inkompatible programmer.

Bruke programmet fra kommandolinjen

Du kan jobbe med Kaspersky-programmet fra kommandolinjen.

Syntaks for kommandolinjen:

```
avp.com <kommando> [parametere]
```

Hvis du vil se hjelpen for kommandolinjesyntaks, skriver du inn følgende kommando:

```
avp.com [ /? | HELP ]
```

Denne kommandoen gir deg en fullstendig liste over kommandoer som er tilgjengelige for å administrere Kaspersky-programmet fra kommandolinjen.

Hvis du vil ha hjelp med syntaksen til en bestemt kommando, skriver du inn en av følgende kommandoer:

```
avp.com <kommando> /?
avp.com HELP <kommando>
```

På kommandolinjen kan du henvise til programmet fra programmets installasjonsmappe eller ved å angi den fullstendige banen til avp.com.

Du kan aktivere eller deaktivere handelseslogging i programmet (opprettelse av sporingsfiler) fra kommandolinjen hvis du allerede har angitt et passord for å beskytte tilgangen til administrering av Kaspersky-programmet i innstillingene til programmet.

Hvis du ikke har angitt et passord i innstillingene til programmet, kan du ikke opprette et passord og aktivere hendelseslogging fra kommandolinjen.

Enkelte kommandoer kan kun utføres under administratorkontoen.

Kontakte Teknisk støtte

Denne delen beskriver hvordan du får teknisk støtte og vilkårene som gjelder for å få støtte.

Få teknisk støtte

Hvis du ikke finner en løsning på problemet i programdokumentasjonen eller i en av de andre informasjonskildene om programmet, anbefaler vi at du tar kontakt med tekniske støtte. Gå inn på teknisk støtte for å kontakte våre eksperter, som vil svare på spørsmålene dine om installasjon og bruk av programmet.

Du bør lese støttereglene før du tar kontakt med Teknisk støtte.

Teknisk støtte er kun tilgjengelig for brukere som har kjøpt et abonnement for bruk av programmet. Teknisk støtte er ikke tilgjengelig for brukere av gratisversjoner.

Hente inn informasjon for Teknisk støtte

Hvis du varsler ekspertene i Teknisk støtte om et problem, vil de eventuelt be deg om å lage en rapport med informasjon om operativsystemet og sende den til Teknisk støtte. Ekspertene i Teknisk støtte kan også be deg om å opprette en sporingsfil. Med sporingsfilen kan du spore utførte programkommandoer trinnvis, og finne ut når i programhendelsene feilen oppsto.

Teknisk støtte vil eventuelt be deg om å endre programinnstillingene midlertidig under diagnostiseringen for feilsøkingsformål, slik at de kan gi bedre støtte for problemer i forbindelse med programmets funksjonalitet. Det gjør du ved å utføre følgende handlinger:

- Innhent utvidet diagnostikkinformasjonen
- Konfigurere de individuelle komponentene i programmet ved å endre spesielle innstillinger som ikke er tilgjengelige i standardgrensesnittet.
- Omkonfigurere lagring og sending av innhentet diagnostikkinformasjon
- Konfigurere oppfanging av nettverkstrafikk og lagring av nettverkstrafikk til en fil

Ekspertene i Teknisk støtte vil gi deg all nødvendig informasjon for å utføre disse handlingene (trinnvise instruksjoner, innstillinger som skal endres, skript, flere kommandolinjefunksjoner, feilsøkingsmoduler, spesialverktøy osv.). De vil også informere deg om hvilke data som vil bli innhentet for feilsøkingsformål. Etter at den utvidede diagnostikkinformasjonen er innhentet, lagres den på brukerens datamaskin. De innhentede dataene sendes ikke automatisk til Kaspersky.

Vi anbefaler at du kun utfører foregående handlinger under veiledning av en ekspert fra Teknisk støtte etter at du har fått beskjed om å gjøre dette. Hvis du selv endrer programinnstillinger som ikke er beskrevet i Hjelpen eller anbefalt av eksperter fra Teknisk støtte, kan det føre til at datamaskinen blir tregere eller at operativsystemet krasjer, redusere datamaskinens beskyttelsesnivå og påvirke tilgjengeligheten og integriteten til den behandlede informasjonen.

Om innholdet og lagringen av tjenestedatafiler

Sporingsfiler og dumpfiler lagres på datamaskinen i ikke-kryptert form i en periode på syv dager etter at datalogging deaktiveres. Sporingsfiler og dumpfiler slettes permanent etter sju dager.

Sporingsfiler lagres i mappen Programdata\Kaspersky Lab.

Sporingsfiler har følgende format: `KAV<version number_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

Sporingsfiler kan inneholde konfidensielle data. Du kan vise innholdet i en sporingsfil ved å åpne den i et tekstredigeringsprogram (for eksempel Notisblokk).

Ytelsessporingsfiler kan åpnes med Performance Analyzer for Windows. Dette verktøyet kan lastes ned fra Microsoft-nettstedet.

Slik aktiverer du sporing

Sørg for at du alltid får veiledning av en Kaspersky-teknisk ekspert når du konfigurerer sporing.

Slik aktiverer du sporing av programmer og ytelse:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i vinduet.

   Vinduet **Støtte** vil da åpne.
3. Klikk på **Støtteverktøy** for å åpne vinduet **Støtteverktøy**.
4. Aktiver og konfigurer sporing av programmer og ytelse ved å følge instruksjonene til en ekspert fra Kasperskys tekniske støtte.
5. Klikk du på **Lagre** for å lagre endringene.

Begrensninger og advarsler

Kaspersky-programmet har en rekke ikke-kritiske bruksbegrensninger.

Begrensninger for bruk av visse komponenter og automatisk behandling av filer

Infiserte filer og skadelige koblinger behandles automatisk i henhold til regler som er opprettet av Kasperskys eksperter. Du kan ikke endre disse reglene manuelt. Reglene kan oppdateres etter oppdatering av databaser og programmoduler. Reglene oppdateres også automatisk for Brannmur, Webkamerabeskyttelse, Application Manager og Inntrengningsbeskyttelse.

Hvis et enhetsskann startes fra My Kaspersky, vil filer behandles automatisk basert på reglene som er spesifisert i programmet. Oppdagede filer på en enhet kan behandles automatisk på anmodning fra My Kaspersky, uten bekreftelse fra deg.

Begrensninger for tilkobling til Kaspersky Security Network

Det kan hende at programmet sender en spørring om informasjon til Kaspersky Security Network. Hvis data fra Kaspersky Security Network ikke kan hentes, tar programmet avgjørelser basert på lokale antivirusdatabaser.

Begrensninger for funksjonen Systemvakt

Beskyttelse mot krypteringsprogrammer (skadelig programvare som krypterer brukerens filer) har følgende begrensninger:

- Den midlertidige systemmappen (Temp) brukes til å støtte denne funksjonen. Hvis stasjonen med den midlertidige mappen ikke har nok diskplass til å opprette midlertidige filer, gis det ikke beskyttelse mot krypteringsprogrammer. Hvis det er tilfellet, vil ikke programmet vise en varsling om at filer ikke er sikkerhetskopiert (ingen beskyttelse).
- Midlertidige filer slettes automatisk når du lukker Kaspersky-programmet eller deaktiverer komponenten Systemvakt.
- Hvis Kaspersky-programmet avsluttes umiddelbart i nødssituasjoner, slettes ikke midlertidige filer automatisk. Du må tømme den midlertidige mappen manuelt for å slette de midlertidige filene. Det gjør du ved å åpne vinduet **Kjør** og skrive inn `%TEMP%` i feltet **Åpne**. Klikk på **OK**.
- Beskyttelse mot krypteringsprogrammer gis kun for filer som ligger på stasjoner som har blitt formatert med filsystemet NTFS.
- Det kan maksimalt gjenopprettes 50 filer per krypteringsprosess.
- Endringer av filer kan ikke overskride en størrelse på totalt 100 MB. Filer med endringer som overskrider denne grensen, kan ikke gjenopprettes.
- Filendringer startet via nettverksgrensesnittet overvåkes ikke.
- Filer kryptert med EFS støttes ikke.
- Du må starte datamaskinen på nytt for å aktivere beskyttelse mot krypteringsprogrammer etter at Kaspersky-programmet er installert.

Skannebegrensninger for krypterte tilkoblinger

På grunn av tekniske begrensninger ved implementering av skannealgoritmer støtter ikke skanning av krypterte tilkoblinger visse filtyper av TLS 1.0-protokollen og nyere versjoner (spesielt NPN og ALPN). Tilkoblinger via disse protokollene kan være begrenset. Nettlesere med støtte for SPDY-protokoller bruker HTTP over TLS-protokollen i stedet for SPDY, selv om den tilkoblede serveren støtter SPDY. Dette påvirker ikke nivået av tilkoblingssikkerhet. Hvis serveren bare støtter SPDY-protokollen og det ikke er mulig å opprette en tilkobling til HTTPS-protokollen, overvåkes ikke tilkoblingen.

Programmet behandler ikke trafikk sendt via utvidelser av HTTP/2-protokollen.

Kaspersky forhindrer utveksling av data via QUIC-protokollen. Nettlesere bruker en standard overføringsprotokoll (TLS eller SSL), uavhengig av om støtte for QUIC-protokollen er aktivert i nettleseren.

Kaspersky overvåker bare krypterte tilkoblinger som det kan dekryptere. Programmet overvåker ikke tilkoblinger som er lagt til på unntakslisten (koblingen **Nettsteder** i vinduet **Nettverksinnstillinger**).

Følgende komponenter dekrypterer og skanner kryptert trafikk som standard:

- Sikker surfing
- Safe Money
- URL-veileder

Kaspersky-programmet dekrypterer kryptert trafikk når brukeren surfer på Google Chrome, hvis utvidelsen for Kaspersky Protection er deaktivert i denne nettleseren.

Kaspersky-programmet overvåker ikke trafikk hvis nettlesere laster inn en webside eller websidens elementer fra en lokal hurtigbuffer i stedet for fra Internett.

Begrensninger på skanning av krypterte tilkoblinger i The Bat-klienten

Siden e-postklienten The Bat bruker sitt eget sertifikatlager, identifiserer Kaspersky-programmet sertifikatet som brukes til å opprette en HTTPS-tilkobling mellom denne klienten og serveren som ikke klarert. For å unngå at dette skjer, må du konfigurere The Bat-klienten til å virke med det lokale sertifikatlageret i Windows.

Begrensninger for unntak fra skanning av krypterte tilkoblinger

Ved skanning av krypterte tilkoblinger til nettsteder som har blitt lagt til som unntak, kan det hende at komponenter som Anti-Banner, URL-veileder og Privat surfing fortsetter å skanne de krypterte tilkoblingene. Komponentene Safe Money og Sikker surfing skanner ikke nettsteder som har blitt lagt til som unntak.

Begrensninger for sikkerhetskopiering og gjenoppretting

Følgende begrensninger gjelder for sikkerhetskopiering og gjenoppretting:

- Nettbasert lagring av sikkerhetskopier blir utilgjengelig ved utskifting av harddisk eller datamaskin. Gå til Kasperskys nettsted for teknisk støtte for å få informasjon om hvordan du gjenoppretter tilkoblingen til Nettlagring etter at du har skiftet ut maskinvare.
- Redigering av servicefilene for sikkerhetskopilageret kan føre til at du mister tilgangen til sikkerhetskopilageret og dermed ikke kan gjenopprette data.

- Programmet oppretter sikkerhetskopier gjennom systemets skyggekopieringstjeneste. Derfor er ikke den frakoblede Outlook-datafilen (.ost) inkludert i sikkerhetskopisettet fordi den ikke er utviklet for å sikkerhetskopieres.

Begrensninger for funksjonaliteten til Hemmelig hvelv

Når et hemmelig hvelv opprettes i filsystemet FAT32, må størrelsen på hemmelig hvelv-filen på stasjonen ikke overstige 4 GB.

Spesifikasjon av kjerneminne ved skanning etter rotsett i Beskyttet nettleser-modus

Når en uklarert modul oppdages i Beskyttet nettleser-modus, åpner en ny nettleserfane med en melding om at skadelig programvare er oppdaget. Hvis dette skjer, anbefaler vi at du avslutter nettleseren og kjører en Fullstendig skann av datamaskinen.

Spesifikasjon av beskyttelse av data på utklippstavlen

Kaspersky-programmet tillater et program tilgang til utklippstavlen i følgende tilfeller:

- Et program i det aktive vinduet forsøker å plassere data på utklippstavlen. Det aktive vinduet er vinduet du bruker i øyeblikket.
- En klarert prosess i et program forsøker å plassere data på utklippstavlen.
- En klarert prosess i et program eller en prosess i det aktive vinduet prøver å motta data fra utklippstavlen.
- En programprosess som tidligere plasserte data på utklippstavlen, forsøker å motta disse dataene fra utklippstavlen.

Detaljer om behandling av infiserte filer av programkomponenter

Ifølge standardinnstillingen kan programmet slette filer som ikke kan desinfiseres. Denne slettingen kan utføres under filbehandling av komponenter som Inntrengningsbeskyttelse, E-post-Antivirus, File Anti-Virus. Filene kan slettes under skanneoppgaver, men også når Systemvakt oppdager skadelige programaktiviteter.

Begrensninger som gjelder for visse komponenter ved programinstallasjon sammen med Kaspersky Fraud Prevention for Endpoints

Driften av følgende komponenter i Kaspersky-programmet er begrenset i Beskyttet nettleser hvis programmet installeres sammen med Kaspersky Fraud Prevention for Endpoints:

- Sikker surfing, unntatt Anti-Phishing
- URL-veileder
- Anti-Banner

Detaljene for autokjøringsprosessen

Autokjøringsprosessen logger resultatene av sine egne handlinger. Data logges i tekstfiler som kalles «kl-autorun-<date><time>.log». Du viser data ved å åpne vinduet **Kjør**. Deretter skriver du inn %TEMP% i feltet **Åpne** og klikker på **OK**.

Alle sporingsfiler lagres i banen til konfigurasjonsfiler som ble lastet ned under autokjøringsprosessen. Data lagres under hele autokjøringsprosessen og slettes permanent når prosessen er fullført. Dataene sendes ikke videre.

Begrensninger for Kaspersky-programmet i Microsoft Windows 10 med modusen Enhetsvakt aktivert:

Driften av følgende funksjoner er delvis begrenset:

- Utklippstavlebeskyttelse
- Nettleserbeskyttelse fra tastatur- og musinngangsemulatorer (inngangsforfalskning)
- Beskyttelse fra eksterne behandlingsprogrammer
- Nettleserbeskyttelse (behandling gjennom API, beskyttelse mot angrep som bruker skadelige meldinger i nettleservinduer, beskyttelse mot købehandling av meldinger)
- Heuristisk analyse (emulering av oppstart av skadelige programmer)

Hvis UMCI-modus er aktivert i Windows, oppdager ikke Kaspersky-programmet skjermlåsere.

Om logging av hendelser relatert til lisensavtalen for sluttbrukere og Kaspersky Security Network i hendelsesloggen i Windows

Hendelser som involverer å godta eller avslå vilkårene i lisensavtalen for sluttbrukere, og også godta og avslå å delta i Kaspersky Security Network, registreres i hendelsesloggen i Windows.

Begrensning av omdømmesjekk av lokale adresser i Kaspersky Security Network

Koblinger til lokale ressurser skannes ikke i Kaspersky Security Network.

Advarsel om programmer som innhenter informasjon

Hvis et program som innhenter informasjon, og sender ut informasjonen for behandling, installeres på datamaskinen, kan det hende Kaspersky-programmet klassifiserer programmet som skadelig programvare. For å unngå dette kan du ekskludere programmet fra skanningen ved å konfigurere Kaspersky-programmet som beskrevet i dette dokumentet.

Advarsel om oppretting av en programinstallasjonsrapport

En installasjonsrapportfil opprettes når programmet installeres på en datamaskin. Hvis programmet ble installert med en feil, lagres en installasjonsrapportfil som du kan sende til Kasperskys tekniske støtte. Du kan se innholdet i installasjonsrapportfilen ved å klikke på lenken i programvinduet. Hvis programmet ble installert, vil installasjonsrapportfilen slettes fra datamaskinen din umiddelbart.

Begrensninger for webkamerakontroll i operativsystemet Microsoft Windows 10 Anniversary Update (RedStone 1)

Etter at programmet er installert i operativsystemet Microsoft Windows 10 Anniversary Update (RedStone 1), vil kontroll av webkameratilgang ikke kunne garanteres før datamaskinen har blitt startet på nytt.

Begrensning for sikkerhetskopiering på Internett og gjenoppretting av data fra sikkerhetskopier

Du kan ikke kjøre en sikkerhetskopieringsoppgave i Kaspersky samtidig som det kjøres datagjenopprettingsoppgaver i Kaspersky Restore Utility på samme datamaskin.

Begrensninger for brannmuren

Brannmuren kontrollerer ikke lokale tilkoblinger som er installert av kontrollerte programmer.

Begrensninger for komponenten Inntrengningsbeskyttelse

Hvis VeraCrypt er installert på datamaskinen, kan det hende Kaspersky-programmet avslutter det når komponenten Programkontroll er aktivert. Oppgrader VeraCrypt til versjon 1.19 eller nyere for å løse dette problemet.

Begrensninger når programmet startes for første gang etter oppgradering fra Microsoft Windows 7 til Microsoft Windows 10

Hvis du har oppgradert fra Microsoft Windows 7 til Microsoft Windows 8 / 8.1 eller Microsoft Windows 10 / RS1 / RS2 / RS3, vil Kaspersky-programmet ha følgende begrenser når det startes for første gang:

- Det er kun Fil-Antivirus (beskyttelse i sanntid) som kjører. Andre programkomponenter kjører ikke.
- Selvforsvar for filer og systemregisteret kjører. Selvforsvar for prosesser kjører ikke.
- Programgrensesnittet er ikke tilgjengelig når du starter maskinen på nytt. Programmet viser et varsel om at enkelte programkomponenter ikke kjører, og at maskinen må startes på nytt etter at tilpasningen til det nye operativsystemet er fullført.
- Det er kun alternativet **Avslutt** som er tilgjengelig i hurtigmenyen under programikonet varslingsområdet.
- Programmet viser ikke varslinger, og velger den anbefalte handlingen automatisk.

Advarsel om feil ved tilpasning av programdrivere ved oppgradering av operativsystemet fra Windows 7 til Windows 10

Oppgradering av Windows 7 til Windows 10 kan føre til en feil ved tilpasning av driverne for Kaspersky-programmet. Drivere tilpasses i bakgrunnen, som betyr at du ikke mottar varsler om fremdriften.

Hvis det oppstår en feil ved tilpasning av driverne, vil du ikke kunne bruke følgende funksjoner i programmet:

- Brannmur

- Trusselvarsling mens operativsystemet laster
- Beskyttelse av programprosesser ved bruk av PPL-teknologien (Protected Process Light) fra Microsoft Corporation

Du kan bruke følgende metoder for å rette feilen:

- Start datamaskinen på nytt og start programtilpasningen fra varslingssenteret.
- Avinstaller programmet og installer det på nytt.

Begrensninger for bruk av Smart Home Monitor

Endring av innstillingene for et Ethernet-nettverk i systemregisteret kan føre til at komponenten Smart Home Monitor viser Ethernet-nettverket i listen over oppdagede trådløse nettverk og viser hvilke enheter som er koblet til dette nettverket.

Begrensninger for skanning av trafikk sendt over HTTPS i nettleseren Mozilla Firefox

I Mozilla Firefox 58.x og nyere versjoner vil programmet ikke skanne trafikk overført over HTTPS-protokollen hvis endringer i nettleserinnstillingene beskyttes av et hovedpassord. Når det oppdages et hovedpassord i nettleseren, viser programmet et varsel med en lenke til en artikkel i kunnskapsbasen. Artikkelen inneholder instruksjoner for hvordan du løser dette problemet.

Hvis HTTPS-trafikk ikke overvåkes, vil funksjonene til følgende komponenter være begrenset:

- Sikker surfing
- Anti-Phishing
- Foreldrekontroll
- Beskyttelse av personvern
- Anti-Banner
- Sikkert datainput
- Safe Money

Begrensninger for Kaspersky Protection-utvidelsen i Google Chrome og Mozilla Firefox

Utvidelsen for Kaspersky Protection fungerer ikke i Google Chrome og Mozilla Firefox hvis Malwarebytes for Windows er installert på datamaskinen din.

Spesielle hensyn ved installasjon av programmet i Microsoft Windows 7 Service Pack 0 og Service Pack 1

Når du installerer programmet i et operativsystem som ikke støtter sertifikater med en digital SHA256-signatur, installerer programmet sitt eget klarerte sertifikat.

Om automatisk testing av funksjonaliteten til Kaspersky-programmer

Kaspersky Lab-programmer, inkludert Kaspersky-programmet, har en spesiell API (programmeringsgrensesnitt for programmet) for automatisk testing av programmets funksjonalitet. Denne API-en skal kun brukes av Kaspersky-utviklere.

Andre informasjonskilder for programmet

Siden for Kaspersky-programmet i kunnskapsbasen

Kunnskapsbasen er en del på nettstedet til Teknisk støtte.

På siden til Kaspersky-programmet i kunnskapsbasen kan du lese artikler som inneholder nyttig informasjon, anbefalinger og svar på vanlige spørsmål om hvordan du kjøper, installerer og bruker programmet.

Artiklene i kunnskapsbasen kan gi svar på spørsmål som gjelder både Kaspersky-programmet og andre Kaspersky-programmer. Artiklene i kunnskapsbasen kan også inneholde nyheter fra Teknisk støtte.

Støtte for Kasperskys programmer i fellesskapet vårt

Du kan få støtte fra brukere og Kaspersky-eksperter i fellesskapet vårt.

I fellesskapet kan du vise eksisterende emner, legge inn kommentarer og opprette nye emner for diskusjon eller for å få hjelp.

Nettverksinnstillinger for samhandling med eksterne tjenester

Kaspersky-programmet bruker følgende nettverksinnstillinger for å samhandle med eksterne tjenester.

Nettverksinnstillinger

Adresse	Beskrivelse
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protokoll: `HTTPS` Port: `443`	Aktivering av programmet.

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protokoll: `HTTPS`
Port: `443`
	Oppdatere databaser og programmoduler.

`downloads.upd.kaspersky.com` Protokoll: `HTTPS` Port: `443`	• Oppdatere databaser og programmoduler. • Verifisere tilgang til Kaspersky-servere. Hvis tilgang til serverne ved hjelp av systemets DNS ikke er mulig, bruker programmet en offentlig DNS. Dette er nødvendig for å sikre at antivirusdatabasene er oppdaterte og et

	datamaskinens sikkerhetsnivå opprettholdes. Kaspersky-programmet bruker følgende liste over offentlige DNS-servere, i følgende rekkefølge: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Forespørsler sendt av programmet kan inneholde adresser til domener og den offentlige IP-adressen til brukeren, fordi programmet oppretter en TCP/UDP-tilkobling til DNS-serveren. Denne informasjonen trengs for eksempel for å validere sertifikatet til en nettressurs ved hjelp av HTTPS. Hvis Kaspersky-programmet bruker en offentlig DNS-server, er databehandlingen underlagt personvernerklæringen til den aktuelle tjenesten. Hvis du vil forhindre at Kaspersky-programmet bruker en offentlig DNS-server, kan du kontakte teknisk støtte og be om en privat oppdatering.
`touch.kaspersky.com` Protokoll: `HTTP`	• Mottar det klarerte klokkeslettet for å sjekke gyldighetsperioden til sertifikatet (TLS-tilkobling). • Advarsel om at tilgang til en nettressurs nektes i nettleseren når Sikker surfing er aktivert.

p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com Protokoll: HTTP Port: 80	Oppdatere databaser og programmoduler.
ds.kaspersky.com Protokoll: HTTPS Port: 443	Bruke Kaspersky Security Network.
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com Protokoll: Any Port: 443, 1443	Bruke Kaspersky Security Network.
click.kaspersky.com redirect.kaspersky.com Protokoll: HTTPS	Følg lenkene fra grensesnittet.

Beskyttelse mot identitetstyveri

Kaspersky Premium-abonnement inkluderer beskyttelse mot identitetstyveri levert av Iris® Powered by Generali, et globalt selskap for beskyttelse mot identitetstyveri og nettsikkerhet.

Beskyttelse mot identitetstyveri er ikke tilgjengelig i enkelte områder. Premium-tjenester som beskrives i denne delen, leveres bare til abonnementets eier. De er ikke tilgjengelige for brukere som eieren har delt et abonnement med.

Tjenester for Beskyttelse mot identitetstyveri

Kundeservice via telefon er ikke tilgjengelig i enkelte regioner.

Kundeservice hos Beskyttelse mot identitetstyveri er åpent jobber døgnet rundt for å hjelpe deg med å ta tilbake den stjålne identiteten og forhindre at slikt tyveri forårsaker ytterligere skade.

- Hjelp hvis du mister eller blir frastjålet lommeboken. Vi vil kontakte banken din for å blokkere og/eller utstede kredittkortene dine på nytt. Hvis du mister førerkortet, ID-kortet eller passet ditt, kontakter vi myndighetene som har utstedt dem for å starte erstatningsprosessen.
- Færre lånetilbud. Vi hjelper deg med å beskytte personopplysningene dine ved å redusere mengden meldinger om godkjente kredittkorttilbud som sendes av svindlere for å stjele identiteten din.
- Fjerning fra adresseliste for reklame. Vi hjelper deg med å redusere antall innkommende e-poster med kredittkorttilbud og anrop fra telefonselgere. Slike tilbud kan være svindlere som prøver å stjele identiteten din.
- Svindelbeskyttelse i tilfeller der det tas opp lån i ditt navn. Hvis identiteten din ble stjålet, kan du sende inn en elektronisk forespørsel om å at alle lån som tas opp i ditt navn det neste året, sjekkes for svindel. Dette forhindrer at den stjålne identiteten din brukes til å ta opp falske lån i ditt navn.
- Fullstendig gjenoppretting av mistede dokumenter. Hvis du eller familiemedlemmer som er inkludert i forsikringen din blir ofre for identitetstyveri eller svindel, vil en av medarbeiderne hjelpe deg med å gjenopprette de personlige dataene dine (etter at en politianmeldelse er levert, et advokatbrev er utstedt til forsikringsselskapet og en erklæring om identitetstyveri er fylt ut). Obs! Denne tjenestens tilgjengelighet avhenger av gjeldende lovgivning i regionen din.
- Løse tvister med kreditorer, varsling og støtte. I regioner der det er mulig, vil vi kontakte avdelingen for svindelforebygging i banken din og sende dem en detaljert rapport om hvert svindeltilfelle. Vi følger opp hver slik saksgang og varsler deg regelmessig om resultatene av rettstvister med spesielle statusrapporter.
- Varsling av politi og myndigheter. Vi hjelper deg med å kontakte politi og myndigheter i saker om identitets, og vil sende en svindelrapport til kreditorene dine.
- Hjelp ved tyveri av sykeforsikringsopplysninger. Hvis sykeforsikringsinformasjonen din blir stjålet, hjelper vi deg (hvis det er mulig i regionen din) med å løse problemet hvis du blir ulovlig fakturert for helsetjenester eller hvis noen på ulovlig vis får legebehandling ved å bruke sykeforsikringen din. Vi vil også sørge for at legeregningene og sykejournalen din rettes opp og, om nødvendig, leie inn vårt eget helsepersonell.
- Hjelp under lange reiser. Hvis identitetstyveri skjedde under en lang reise (over 100 miles (ca. 160 km) fra der du bor), hjelper vi deg med å kjøpe flybilletter, bestille hotell og leie en bil.

- Kontantbeløp ved uventede omstendigheter. Hvis identitetstyveri skjedde over 100 miles (ca. 160 km) fra der du bor, gir vi deg et kontantbeløp på 500 dollar (ca. 4900 kroner). Alle utgifter innenfor dette beløpet er etter ditt eget skjønn. Du må ha et gyldig kredittkort for å benytte deg av denne tjenesten. Dersom du ikke har oppgitt et gyldig kredittkort, og likevel mottok et slikt kontantbeløp, skal beløpet faktureres kredittorganisasjonen din til fordel for forsikringsselskapet innen 30 dager fra datoen da godtgjørelsen ble gjort tilgjengelig for deg, og du skal tilbakebetale gjelden til kredittorganisasjonen innen 45 dager etter at du mottok beløpet. Hvis du ikke har betalt gjelden etter at denne perioden utløper, skal du betale renter på beløpet med en månedlig rente på 1.5 %. Forsikringsselskapet forbeholder seg retten til å nekte deg et kontantbeløp hvis du ikke har et gyldig kredittkort.

De nevnte tjenestenes tilgjengelighet avhenger av regionen du befinner deg i.

Forsikring mot identitetstyveri

Ved å benytte deg av forsikring mot identitetstyveri kan du beskytte deg mot utgifter knyttet til å gjenopprette personopplysninger. Unn deg å sove i ro, ved å føle deg trygg på at du vil få 1 million dollar til å gjenopprette personopplysninger og dekke utgifter hvis du noen gang blir frastjålet eller mister personopplysningene dine.

Forsikring mot identitetstyveri gis som en del av hovedpolisen fra Generali US Branch, til fordel for Generali Global Assistance, Inc. Disse vilkårene og betingelsene er kun til informasjon og inkluderer ikke alle klausuler, betingelser og unntak i forsikringskontrakten. Forsikringsdekning gis kanskje ikke i enkelte jurisdiksjoner. Personer som deltar i forsikringsprogrammet må oppgi detaljert informasjon om betingelser og ytelser direkte i forsikringsavtalen. Generali US Branch (New York, NY; NAIC # 11231) opererer under følgende navn: Generali Assicurazioni Generali S.P.A. (U.S. Branch) i California, Assicurazioni Generali – U.S. Branch i Colorado, Generali U.S. Branch DBA The General Insurance Company of Trieste & Venice i Oregon og The General Insurance Company of Trieste and Venice – U.S. Branch i Virginia. Generali US Branch er godkjent eller lisensiert til å gjøre forretninger i alle stater og Washington D.C.

De ovennevnte funksjonenes tilgjengelighet avhenger av regionen. Du kan bare bruke dem med et betalt abonnement.

Hjelp med forebygging av svindel

Svindlere bruker en rekke metoder for å stjele pengene dine. De kan sende deg falske fakturaer eller be deg om å betale for en falsk bestilling på nett. Hvis du er i tvil om hvorvidt et bestemt tilbud er legitimt, kan du ringe oss så vi kan sjekke det.

Forebygging av og støtte for svindel omfatter:

- ScamAssist. Hvis du mottar en melding eller et tilbud som ser mistenkelig ut eller for godt til å være sant, vil medarbeiderne til ScamAssist analysere meldingen eller tilbudet og advare deg hvis det viser seg å være svindel, og dermed forhindre tyveri av pengene og personopplysningene dine.

Forsikringstjenesteleverandøren er ikke ansvarlig for tilgjengeligheten, sikkerheten, nøyaktigheten og effektiviteten til bestemte metoder, produkter, verktøy eller ressurser som brukes som en del av svindelforebyggings- og støttetjenesten. Du påtar deg ansvaret for å bruke svindelforebyggings- og støttetjenesten.

Ordliste

Aktivering av programmet

Veksle programmet til fullstendig fungerende modus. Programmet aktiveres av brukeren under eller etter installasjon av programmet. Brukeren må ha en aktiveringskode for å aktivere programmet.

Antivirusdatabaser

Disse databasene inneholder informasjon om datasikkerhetstruslene som Kaspersky kjenner til på utgivelsestidspunktet for databasene. Oppføringene i disse databasene gjør det mulig å oppdage skadelige koder i skannede objekter. Databasene opprettes av ekspertene til Kaspersky, og oppdateres hver time.

Beskyttelseskomponenter

Hovedelementene i Kaspersky-programmet, som beskytter datamaskinen mot bestemte trusseltyper (for eksempel Anti-Spam, Anti-Phishing). Alle komponentene er relativt uavhengige av hverandre, slik at de kan deaktiveres og konfigureres individuelt.

Beskyttet Nettleser

En spesifikk driftsmodus for en standardnettleser spesielt beregnet på finansaktiviteter og netthandel. Beskyttet nettleser garanterer sikkerheten til konfidensielle data som du angir på nettstedene til banker og betalingssystemer, for eksempel bankkortnumre og passord for nettbanktjenester. Den forhindrer også at penger blir stjålet når du betaler på nett.

Blokkering av et objekt

Nekter tilgang til et objekt fra eksterne programmer. Et blokkert objekt kan ikke bli lest, kjørt, endret eller slettet.

Database med skadelige nettadresser

Liste over nettadresser der innholdet kan betraktes som farlig. Listen er opprettet av Kasperskys spesialister, og oppdateres regelmessig og er inkludert i programpakken for Kaspersky.

Databasen med phishing-lenker og falske kryptobørser

Liste over nettadresser som er definert som phishing-nettadresser av spesialister fra Kaspersky. Databasen blir jevnlig oppdatert og er del av Kasperskys programpakke.

Digital signatur

En kryptert blokk med data som er innebygd i et dokument eller et program. En digital signatur brukes til å identifisere forfatteren av dokumentet eller programmet. Forfatteren av dokumentet eller programutvikleren må ha et digitalt sertifikat som beviser sin identitet, for å kunne opprette en digital signatur.

Ved hjelp av en digital signatur kan du kontrollere datakilden og dataintegriteten og beskytte deg mot svindel.

Diskens oppstartssektor

En oppstartssektor er et bestemt sted på en datamaskins harddisk, diskett eller annen datalagringsenhet. Den inneholder informasjon om diskens filsystem og et oppstartsprogram som har som oppgave å starte operativsystemet.

Det finnes mange virus som infiserer oppstartssektorer, som dermed kalles oppstartsvirus. Med programmet fra Kaspersky kan du skanne oppstartssektorer for virus og desinfisere dem hvis en infeksjon blir funnet.

Falske positive

Situasjon som oppstår når programmet fra Kaspersky betrakter et ikke-infisert objekt som infisert fordi koden ligner på koden fra et virus.

Filmaske

Representasjon av et filnavn ved hjelp av jokertegn. De to standard jokertegnene som brukes i filmasker, er * og ?, der * representerer et vilkårlig antall tegn og ? står for et enkelttegn.

Hemmelig hvelv

Et datahvelv er et spesielt datalagringsområde der filer lagres i kryptert form. Det kreves passord for å få tilgang til slike filer. Hemmelige hvelv skal hindre uautorisert tilgang til brukerdata.

Heuristisk analyseprogram

En teknologi som oppdager trusler som ennå ikke er lagt til i databasene til Kaspersky. Det heuristiske analyseprogrammet finner objekter med en atferd som kan utgjøre en sikkerhetstrussel i operativsystemet. Filer oppdaget av det heuristiske analyseprogrammet, anses som potensielt infiserte. Et objekt kan for eksempel anses som potensielt infisert hvis det inneholder sekvenser med kommandoer som er typiske for skadelige objekter (åpne fil, skriv til fil).

Hypervisor

Et program som støtter parallell kjøring av flere operativsystemer på én datamaskin.

iChecker-teknologi

En teknologi som gjør at hastigheten på antivirusskanning kan økes ved å ekskludere objekter som ikke har blitt endret siden forrige skanning, forutsatt at skanneparameterne (antivirusdatabasen og innstillingene) ikke er endret. Informasjonen for hver fil er lagret i en spesiell database. Denne teknologien brukes i både sanntidsbeskyttelse og skann på forespørsel.

Eksempel: Du har en arkivfil som er skannet av et Kaspersky-program, og ble tildelt statusen *ikke infisert*. Neste gang vil programmet hoppe over dette arkivet, med mindre det har blitt endret, eller skanneinnstillingene er endret. Hvis du har endret innholdet i arkivet ved å legge til et nytt objekt, endret innstillinger for skann eller oppdaterte programdatabasene, blir arkivet skannet på nytt.

Begrensninger i iChecker-teknologien:

- Denne teknologien virker ikke med store filer, ettersom det er raskere å skanne en fil enn å sjekke om den er modifisert siden forrige skann.
- Teknologien støtter et begrenset antall formater.

Infisert objekt

Et objekt der en del av koden er helt lik koden til en kjent ondsinnet programvare. Kaspersky anbefaler ikke at du bruker slike objekter.

Inkompatibelt program

Et antivirusprogram fra en tredjeparts utvikler eller et program fra Kaspersky Lab som ikke støtter administrering gjennom Kaspersky.

Karantene

Et spesifikt lager som brukes til å lagre sikkerhetskopier av filer som er endret eller slettet under desinfisering. Kopier av filene lagres i et spesielt format som ikke er farlig for datamaskinen.

Kaspersky Security Network (KSN)

Den skybaserte kunnskapsbasen til Kaspersky, som inneholder informasjon om omdømmet til programmer og nettsteder. Bruk av data fra Kaspersky Security Network gjør det mulig for programmene i Kaspersky å reagere raskere når det oppdages trusler, øker ytelsen til noen av beskyttelseskomponentene og reduserer faren for falske positive.

Kasperskys oppdateringsservere

Kasperskys HTTP-servere som oppdaterte antivirusdatabaser og programvaremoduler lastes ned fra.

Klareringsgruppe

En gruppe der Kaspersky-programmet plasserer et program eller en prosess basert på følgende kriterier: registrering av en digital signatur, omdømme i Kaspersky Security Network, klareringsnivået til programkilden samt potensiell fare i forbindelse med handlinger som utføres av programmet eller prosessen. Basert på klareringsgruppen til et program, kan Kaspersky begrense handlingene til programmet i operativsystemet.

I Kaspersky-programmet brukes følgende klareringsgrupper: Klarert, Lavt begrenset, Høyt begrenset eller Uklarert.

Klarert prosess

En programvareprosess der handlinger som involverer filer ikke begrenses av Kaspersky-programmet i sanntid. Når mistenkelig aktivitet oppdages i en klarert prosess, fjerner Kaspersky-programmet prosessen fra listen over klarerte prosesser, og blokkerer handlingene den utfører.

Komprimert fil

En komprimert kjørbar fil som inneholder et utpakkingsprogram og instruksjoner for kjøring for operativsystemet.

Mulig spam

Melding som ikke utvetydig kan anses som spam, men som har flere spamattributter (f.eks. bestemte typer e-post og reklamemeldinger).

Oppdatering

Utbytting/tillegging av nye filer (database- eller programmoduler) mottatt fra Kasperskys oppdateringsservere.

Oppdateringspakke

En filpakke som brukes til å oppdatere databaser og programmoduler. Et Kaspersky-program kopierer oppdateringspakker fra Kasperskys oppdateringsservere til datamaskinen. Deretter blir de automatisk installert og brukt.

Oppgave

Funksjonene i Kaspersky-programmet implementeres i form av oppgaver, for eksempel et Fullstendig skann eller en Oppdateringsoppgave.

Oppgaveinnstillinger

Programinnstillinger som er spesifikke for hver oppgavetype.

Oppstartsobjekter

Samlingen programmer som er nødvendig for å starte og bruke operativsystemet og programvare installert på datamaskinen på riktig måte. Disse objektene blir kjørt hver gang operativsystemet starter. Det finnes virus som spesielt er i stand til å infisere autokjøringsobjekter, noe som f.eks. kan føre til at tilgang til operativsystemet blir blokkert.

Phishing

En type Internett-svindel som prøver å få uautorisert tilgang til brukerens konfidensielle data.

Potensielt infisert objekt

Et objekt der koden inneholder deler av modifisert kode fra en kjent trussel, eller et objekt med lignende atferd som en trussel.

Programmoduler

Filer som er med i installasjonspakken fra Kaspersky og som sørger for kjøring av hovedoppgavene i det tilsvarende programmet. En bestemt programmodul tilsvarer hver type oppgave som utføres av programmet (beskyttelse, skanning, oppdatering av antivirusdatabaser og programmoduler).

Protokoll

Et klart definert og standardisert sett av regler som styrer samhandlingen mellom en klient og en server. Velkjente protokoller og tjenestene i tilknyttet dem omfatter blant annet HTTP, FTP, og NNTP.

Rotsett

Et program eller et sett programmer som er utviklet for å skjule spor etter inntrengere eller skadelige programmer i operativsystemet.

I Windows-baserte systemer betyr rotsett vanligvis et program som trenger inn i operativsystemet og fanger opp systemfunksjoner (Windows API). Oppfanging og endring av API-funksjoner på lavt nivå er hovedmetoden som disse programmene bruker til å trenge inn i operativsystemet. Et rotsett kan også maskere prosesser, mapper og filer som er lagret på en diskstasjon, samt registernøkler, hvis de er beskrevet i konfigurasjonen til rotsettet. Mange rotsett installerer sine egne drivere og tjenester i operativsystemet (de er også «usynlige»).

Sårbarhet

En svakhet i et operativsystem eller et program, som kan utnyttes av skadelig programvare for å trenge inn på operativsystemet eller i programmet og skade dem. Hvis det finnes mange sårbarheter i et operativsystem, vil det bli upålitelig fordi virus som trenger inn på operativsystemet, kan føre til avbrudd i operativsystemet og i installerte programmer.

Sikkerhetskopiering og gjenoppretting

Oppretter sikkerhetskopier av data som er lagret på datamaskinen. Sikkerhetskopier opprettes for å hindre tap av data som følge av tyveri, maskinvarefeil eller hackerangrep.

Sikkerhetsnivå

Sikkerhetsnivået defineres som en forhåndsdefinert samling av innstillinger for en programkomponent.

Skript

Et lite dataprogram eller en uavhengig del av et program (funksjon), som vanligvis er utviklet for å utføre en liten og bestemt oppgave. Det brukes i de fleste tilfeller med programmer innebygd i hypertekst. Skript kjøres for eksempel når du åpner spesifiserte nettsteder.

Hvis sanntidsbeskyttelse er aktivert, sporer programmet oppstart av skripter, hindrer og skanner dem for virus. Avhengig av skanneresultatet, kan du blokkere eller tillate kjøring av et skript.

Spam

Uønskede masseutsendelser av e-post, for det meste med annonser.

Sporing

Kjører programmet i feilsøkingsmodus, etter hver kommando er utført, programmet er stanset og resultatet av dette trinnet vises.

Tastelogger

Et program som brukes til skjult logging av informasjon om tastene som brukeren trykker på. Tasteloggere fanger opp tastetrykk.

Trafikkskanning

Sanntidsskanning som bruker informasjon fra gjeldende (siste) versjon av databasene ved skanning av objekter som overføres over alle protokoller (f.eks. HTTP, FTP osv.).

Trusselnivå

En oversikt som viser sannsynligheten for at et program vil utgjøre en trussel for operativsystemet. Trusselnivået beregnes ved hjelp av en heuristisk analyse basert på to typer kriterier:

- Statiske (som f.eks. informasjon om den kjørbare filen til et program: størrelse, dato for opprettelse, osv.)
- Dynamiske – som brukes samtidig som programmets drift simuleres i et virtuelt miljø (analyse av programmets samspill med systemfunksjoner)

Trusselnivåer gjør det mulig å oppdage aktivitet som er typisk for skadelig programvare. Et lavt trusselnivå betyr at programmet kan utføre flest mulig handlinger i operativsystemet.

Ukjent virus

Et nytt virus som det ikke er noen informasjon om i databasene. Vanligvis oppdages ukjente virus av programmet i objekter ved hjelp av den heuristiske analysen. Disse objektene klassifiseres som muligens infisert.

Utnyttelse

En programvarekode som bruker en sårbarhet i systemet eller programvaren. Utnyttelser brukes ofte til å installere skadelig programvare på datamaskinen uten at brukeren vet det.

Virus

Et program som infiserer andre programmer ved å legge til koder i dem for å få kontroll over programmet ved kjøring av infiserte filer. Denne enkle definisjonen gjør det mulig å finne hovedhandlingen som utføres av alle typer virus, nemlig infisering.

Informasjon om tredjeparts kode

Informasjon om tredjeparts kode oppbevares i filen legal_notices.txt og lagres i programmets installasjonsmappe.

Notater om varemerker

Registrerte varemerker og tjenestemerker tilhører sine respektive eiere.

Adobe, Acrobat og Reader er registrerte varemerker eller varemerker for Adobe Systems Incorporated i USA og/eller andre land.

Apple, macOS, App Store og Safari er varemerker som tilhører Apple Inc., registrert i USA og andre land og regioner.

Dropbox er et varemerke som tilhører Dropbox, Inc.

Google, Google Chrome, Google Play, Chromium, SPDY, YouTube og Android er varemerker som tilhører Google LLC

Intel, Celeron og Atom er varemerker som tilhører Intel Corporation i USA og i andre land.

IOS er registrerte varemerker eller varemerker for Cisco Systems, Inc. og/eller deres tilknyttede selskaper i USA og visse andre land.

Java og JavaScript er registrerte varemerker som tilhører Oracle og/eller deres tilknyttede selskaper.

Linux er et varemerke som tilhører Linus Torvalds, og er registrert i USA og andre land.

LogMeIn Pro og Remotely Anywhere er varemerker som tilhører LogMeIn, Inc.

Mail.ru er et varemerke som tilhører Mail.ru LLC.

Microsoft, Windows, Windows Mail, Internet Explorer, Outlook, PowerShell, Bing og Skype er varemerker som tilhører Microsoft-konsernet.

Mozilla, Thunderbird og Firefox er varemerker som tilhører Mozilla Foundation.

VMware er et registrert varemerke som tilhører VMware, Inc. i USA og/eller andre jurisdiksjoner.

Liste over tjenester som passordet sendes til når en QR-kode skannes

Når du skanner en QR-kode med en Android-enhet, sendes et engangspassord for å aktivere programmet på smarttelefonen til Google Play og AppsFlyer.

Vinduet Oppgrader

Prøveversjon

Koblingen starter overgangen til prøveabonnementet.

Kjøp aktiveringskode

Når du klikker på denne knappen, åpnes websiden til en nettbutikk, der du kan kjøpe et abonnement.

Skriv inn aktiveringskode

Klikk på denne lenken for å kjøre aktiveringsveiviseren for programmet.

Vinduet Oppgrader

Kjøp aktiveringskode

Klikk på denne lenken for å peke nettleseren til nettbutikken der du kan kjøpe et abonnement på programmet du bytter til.

Skriv inn aktiveringskode

Klikk på denne lenken for å kjøre aktiveringsveiviseren for programmet.

Prøveversjon

Klikk på knappen for å bytte til en prøveversjon av et annet program.

Aktivere programmet med en reserve-aktiveringskode

Hvis du vil bruke en reserve-aktiveringskode, klikker du på **Neste**-knappen.

Hvis lisensen ikke har utløpt enda, kan du bruke aktiveringskoden du benyttet til å aktivere programmet tidligere, på en annen datamaskin.

Du avbryter aktiveringen av programmet ved å klikke på koblingen **Avbryt**.

Avbryt

Klikk på denne koblingen for å avbryte bruk av reserve-aktiveringskoden og gå tilbake til vinduet **Lisensiering**.

Vinduet Angi aktiveringskode

Felter for inntasting av et programs aktiveringskoder

Du kan ha mottatt en aktiveringskode, enten på e-post eller i en fysisk butikk. En aktiveringskode består av fire grupper med tegn (for eksempel **ABA9C-CDEFG-ABCBC-ABC2D**).

Gjenopprett abonnementet fra kontoen din

Når du klikker på denne lenken, åpnes et vindu med skjemaet som lar deg koble enheten til My Kaspersky-kontoen din for å aktivere et abonnement som er lagret på kontoen.

Hvor kan jeg få tak i en aktiveringskode?

Når du klikker på **Hvor kan jeg få tak i en aktiveringskode?**, åpnes et nettleservindu med detaljert informasjon om hvordan du aktiverer programmet ved hjelp av en aktiveringskode.

Kjøp abonnement

Klikk på denne lenken for å åpne et nettleservindu med eStore, der du kan kjøpe et abonnement.

Aktiver

Klikk på denne knappen for å begynne å aktivere programmet ved å bruke den angitte aktiveringskoden.

Aktiveringskoden samsvarer med koden til et annet program

Dette vinduet åpnes hvis den angitte aktiveringskoden er ment for et annet program. Du kan starte å bruke dette programmet nå eller etter at abonnementet for Kaspersky-programmet utløper.

Avbryt

Klikk på denne koblingen for å avbryte aktivering av programmet.

Fortsett

Ved å klikke på denne knappen starter installasjon og aktivering av programmet som den angitte aktiveringskoden tilsvarer.

Informasjon om nettstedkategorier

Du kan se beskrivelser av nettstedkategorier via følgende lenke.

Slik konfigurerer du DNS over HTTPS-beskyttelse

Når du skriver inn et nettstednavn i adressefeltet, sender nettleseren forespørselen din til en DNS-server. DNS-serveren fastsetter IP-adressen til nettstedet du har forespurt. Data overføres fra datamaskinen din til DNS-serveren ved å bruke en vanlig ukryptert tekstprotokoll. Inntrengere kan fange opp informasjon om nettsteder du besøker, og misbruke den. For å forhindre at dette skjer, bør denne informasjonen overføres over den sikre HTTPS-protokollen. Serveren som mottar og analyserer slike forespørsler, kalles en DoH-server (eller DNS over HTTPS).

Kaspersky mottar automatisk data om hvilken DoH-server som brukes i Mozilla Firefox. Hvis du har lagt til en DoH-server manuelt i Kaspersky-programmet, og du vil at DNS-data skal overføres gjennom denne DoH-serveren, må du legge til denne serveren i innstillingene for Mozilla Firefox. Hvis du vil ha informasjon om konfigurering av DoH-serveren, ser du hjelpesidene i Mozilla Firefox.

Legg til en DoH-server

Slik legger du til en DoH-server:

1. Åpne hovedvinduet.
2. Klikk på -knappen nederst i hovedvinduet.

   Vinduet **Innstillinger** vil da åpne.
3. I delen **Ekstra** velger du underkategorien **Nettverk**.

   Vinduet **Nettverksinnstillinger** vil da åpne.
4. I seksjonen **Trafikkbehandling** klikker du på lenken **Administrer DoH-servere** for å åpne vinduet **DoH-servere**.
5. Klikk på **Legg til**.
6. Skriv inn navnet eller IP-adressen til DoH-serveren i vinduet som åpnes og klikk på **Legg til**.

DoH legges til i listen.

Vinduet Informasjon om gjeldende lisens oppdaget

Ja, bruk <program>

Hvis du velger dette alternativet, lukkes aktiveringsveiviseren. Programmet kjører med det oppdagede aktive abonnementet. Hvis det oppdages et abonnement på Kaspersky Standard eller Kaspersky Plus, startes migreringsveiviseren.

Nei, fortsett veiviseren og oppgi ny aktiveringskode

Hvis du velger dette alternativet, vil aktiveringsveiviseren fortsette med aktiveringen av programmet. Du må angi en ny aktiveringskode som er gyldig for dette programmet.

Vinduet Registrering

I dette vinduet angir du registreringsdata som er nødvendig for å kontakte Teknisk støtte.

Ingen Internett-tilkobling er tilgjengelig

Dette vinduet vises hvis du ikke kan aktivere programmet på grunn av problemer med Internett-tilkoblingen.

Prøv på nytt

Hvis du klikker på denne koblingen, vil aktiveringsveiviseren prøve å aktivere programmet på nytt. Hvis problemene med Internett-tilkobling er midlertidig, kan nye forsøk være vellykkede.

Delen Velg hvor du vil plassere gjenopprettede filer

Opprinnelig mappe

Hvis dette alternativet er aktivert, gjenoppretter programmet filene fra den opprinnelige mappen.

Angitt mappe

Hvis dette alternativet er aktivert, gjenoppretter programmet filene i mappen som er angitt i feltet **Velg mappe**.

Velg mappe

Feltet inneholder banen til mappen som filene skal gjenopprettes i.

Dette feltet er tilgjengelig hvis alternativet **Angitt mappe** er valgt.

Bla gjennom

Denne knappen åpner vinduet **Velg hvor du vil plassere gjenopprettede filer**. I dette vinduet kan du velge mappen som filene skal gjenopprettes i.

Knappen er tilgjengelig hvis alternativet **Angitt mappe** er valgt.

Hvis filnavn ikke samsvarer

I denne rullegardinlisten kan du velge en handling som skal utføres av programmet når målmappen for filen som blir gjenopprettet, allerede inneholder en fil med samme navn:

- **spør** – hvis det oppdages samsvarende filnavn, blir du bedt om å velge ett av disse alternativene: Erstatte filen med sikkerhetskopien, lagre begge filene eller ikke gjenopprette filen.
- **erstatt filen med sikkerhetskopien** – Kaspersky-programmet sletter den eksisterende filen og erstatter den med den gjenopprettede filen fra sikkerhetskopien.
- **lagre begge filene** – Kaspersky-programmet beholder den eksisterende filen og lagrer den gjenopprettede filen fra sikkerhetskopien med et nytt navn i samme mappe.
- **ikke gjenopprett denne filen** – Kaspersky-programmet beholder den eksisterende filen og gjenoppretter ikke filen med samme navn fra sikkerhetskopien.

Gjenopprett

Klikk på denne knappen for å starte gjenoppretting av filer fra sikkerhetskopier.

Aktiveringsfeil

Programaktivering mislyktes. Klikk på koblingen **Årsaker og mulige løsninger** for å vise informasjon om problemet i kunnskapsbasen.

Årsaker og mulige løsninger

Klikk på denne koblingen for å gå til en artikkel i kunnskapsbasen, der du finner informasjon om årsaken til feilen og mulige løsninger.

Koblinger til artikler i kunnskapsbasen er eventuelt ikke tilgjengelige for alle feil.

Avbryt

Klikk på denne koblingen for å avbryte aktivering av programmet.

Bytte til et annet program

Klikk på **Neste** for å fortsette med migrasjonsveiviseren. Migrasjonsveilederen installerer programmet som samsvarer med den angitte aktiveringskoden (Kaspersky Standard eller Kaspersky Plus).

Hvis abonnementet ditt for Kaspersky ikke har utløpt ennå, kan du bruke aktiveringskoden for Kaspersky på en annen datamaskin.

Hvis du vil avbryte migrasjonen til Kaspersky Standard eller Kaspersky Plus, klikker du på koblingen **Avbryt**.

Avbryt

Klikk på denne koblingen for å avslutte migrasjonsveiviseren og gå tilbake til forrige trinn.

Kontroller at aktiveringskoden du angir, ikke er aktiveringskoden for et abonnement.

Kontroller at aktiveringskoden du angir som reservekode, ikke er ment for abonnementsbasert bruk av programmet. Betaling for abonnementsbasert bruk av programmet innkreves når du får tak i abonnementet. Hvis du har kjøpt et abonnement for Kaspersky, må du ikke bruke programmet under gjeldende lisens. Aktivere i stedet programmet med en abonnementsaktiveringskode.

Frem til lisensen utløper kan du bruke en aktiveringskode som allerede er i bruk, til å aktivere programmet på en annen datamaskin.

Vinduet Kjøresekvens

Programkjøresekvens

Listen inneholder informasjon om programmer som er startet av det valgte programmet (underordnede programmer). Som standard sorteres underordnede programmer etter tidspunktet de ble startet, med det tidligste tidspunktet først.

Start

Denne kolonnen viser tidspunktet da det underordnede programmet ble startet.

Prosess-ID

Denne kolonnen viser prosess-IDen til det underordnede programmet.

Program

Denne kolonnen viser navnet på det underordnede programmet.

Klareringsgruppe

Denne kolonnen viser klareringsgruppen som programmet tilhører:

- **Klarert**. Programmet kjører uten begrensninger, men kontrolleres av File Anti-Virus.
- **Lavt begrenset**. Programmet gis ikke tilgang til brukerens personlige data og innstillinger, og har heller ikke tillatelse til å redigere offentlige data. Ethvert forsøk på å endre systemdata eller utføre privilegerte handlinger krever tillatelse fra brukeren. Nettverksaktiviteten til slike programmer er begrenset.
- **Høyt begrenset**. Programmet gis ikke tilgang til brukerens personlige data og innstillinger, samt til offentlige data og systemdata. Eventuelle privilegerte handlinger krever tillatelse fra brukeren. Nettverksaktiviteten til slike programmer er blokkert.
- **Uklarert**. Alle aktiviteter til slike programmer er fullstendig blokkert.

Kategorien Kjører

Liste over aktive programmer

Listen inneholder programmer og prosesser som kjører på datamaskinen for øyeblikket.

Høyreklikk for å åpne hurtigmenyen til en kolonneoverskrift. I hurtigmenyen kan du konfigurere hvordan kolonner med tilleggsinformasjon om programmer og prosesser skal vises:

- Navnet på den kjørbare filen til programmet eller prosessen
- Detaljer om programleverandøren
- Prosess-ID
- Banen til programmets kjørbare fil
- Navnet på brukeren som har startet programmet eller prosessen
- Tidspunktet for opprettelse og start av programmet eller prosessen
- Innstillinger for automatisk kjøring i programmet

Elementet **Gjenopprett standard kolonneoppsett** lar deg gjenopprette tabellens standardutseende.

Høyreklikk på raden til programmet eller prosessen for å åpne hurtigmenyen. Fra hurtigmenyen kan du utføre følgende handlinger:

- Åpne vinduet **Programregler**, der du kan konfigurere regler for begrensing av programaktiviteter.
- Vise rekkefølgen prosessene ble startet i, fra vinduet **Kjøresekvens**.
- Flytte programmet til en annen klareringsgruppe.
- Bruke standardinnstillinger for rettigheter i et program.
- Avslutt prosessen.
- Åpne mappen som inneholder den kjørbare filen til programmet.

Vis

Fra rullegardinlisten kan du aktivere visning av systemprosesser og prosesser som er startet av Kaspersky:

- **Vis systemprosesser**. Hvis du velger dette alternativet, vil den generelle listen over programmer og prosesser inneholde prosesser som er nødvendige for at operativsystemet skal fungerer riktig.
- **Vis <PRODUCT>-prosesser**. Hvis du velger dette alternativet, vil den generelle listen over programmer og prosesser vise prosesser som er startet av Kaspersky.

Fra rullegardinlisten kan du velge visningsmodus for programmer og prosesser:

- **Vis som liste**. Hvis du velger dette alternativet, vil programmer og prosesser vises som en liste.
- **Trevisning**. Hvis du velger dette alternativet, vil programmene og prosessene vises hierarkisk, basert på rekkefølgen prosessene ble startet i.

Program

Denne kolonnen viser navnet på et program eller en prosess.

Digital signatur

Denne kolonnen viser informasjon som angir om programmet har en digital signatur og hvem som eier denne signaturen.

Klareringsgruppe

Denne kolonnen viser klareringsgruppen som programmet tilhører. Avhengig av klareringsgruppen som programmet tilhører, inneholder kolonnen følgende ikoner:

- Et rødt ikon angir at programmet er inkludert i gruppen Uklarert.
- Et rosa ikon angir at programmet er inkludert i gruppen Høyt begrenset.
- Et gult ikon angir at programmet er inkludert i gruppen Lavt begrenset.
- Et grønt ikon angir at programmet er inkludert i gruppen Klarert.
- Noen spesialiserte systemprosesser (for eksempel System eller MemCompression) sorteres ikke i klareringsgrupper og kontrolleres ikke av Kaspersky. Slike prosesser vises som et grått ikon og merkes som «Ukjent».

Popularitet

Denne kolonnen viser programmets popularitet blant deltakerne i Kaspersky Security Network (KSN). Popularitetsnivået avhenger av antallet KSN-deltakere som bruker programmet.

CPU

Denne kolonnen viser gjeldende andel av CPU-ressurser som programmet eller prosessen tar opp.

Minne

Denne kolonnen viser gjeldende andel av minnet (RAM) som programmet eller prosessen tar opp.

Disk

Denne kolonnen viser den totale hastigheten for lesing og skriving av data for programmet eller prosessen.

Nettverk

Denne kolonnen viser programmets totale hastighet ved overføring av data via nettverksgrensesnittet.

Avslutt prosess

Ved å klikke på denne knappen avslutter du programmet som er markert i listen.

Kategorien Kjør ved oppstart

Liste over programmer som kjører ved oppstart

Listen inneholder programmer som startes når operativsystemet startes.

Høyreklikk for å åpne hurtigmenyen til en kolonneoverskrift. I hurtigmenyen kan du konfigurere måten kolonner vises på i tabellen. Elementet **Gjenopprett standard kolonneoppsett** lar deg gjenopprette tabellens standardutseende.

Høyreklikk på raden til programmet eller prosessen for å åpne hurtigmenyen. Fra hurtigmenyen kan du utføre følgende handlinger:

- Åpne vinduet **Programregler**, der du kan konfigurere regler for begrensing av programaktiviteter.
- Flytte programmet til en annen klareringsgruppe.
- Bruke standardinnstillinger for rettigheter i et program.
- Åpne mappen som inneholder den kjørbare filen til programmet.

Program

Denne kolonnen viser navnet på programmet som starter når operativsystemet startes.

Status

Denne kolonnen viser programmets status: *Kjører* eller *Stoppet*.

Digital signatur

Denne kolonnen viser informasjon som angir om programmet har en digital signatur og hvem som eier denne signaturen.

Klareringsgruppe

Denne kolonnen viser klareringsgruppen som programmet tilhører. Avhengig av klareringsgruppen som programmet tilhører, inneholder kolonnen følgende ikoner:

- Et rødt ikon angir at programmet er inkludert i gruppen Uklarert.
- Et rosa ikon angir at programmet er inkludert i gruppen Høyt begrenset.
- Et gult ikon angir at programmet er inkludert i gruppen Lavt begrenset.
- Et grønt ikon angir at programmet er inkludert i gruppen Klarert.
- Noen spesialiserte systemprosesser (for eksempel System eller MemCompression) sorteres ikke i klareringsgrupper og kontrolleres ikke av Kaspersky. Slike prosesser vises som et grått ikon og merkes som «Ukjent».

Popularitet

Denne kolonnen viser programmets popularitet blant deltakerne i Kaspersky Security Network (KSN). Popularitetsnivået avhenger av antallet KSN-deltakere som bruker programmet.

Siste kjøring

Denne kolonnen viser det siste tidspunktet da programmet ble startet.

Nettverket du har definert som hjemmenettverket, er faktisk offentlig

Når du kobler til et offentlig trådløst nettverk, for eksempel på en kafé, overføres data uten kryptering. Det betyr at passord, brukernavn, meldinger og annen konfidensiell informasjon blir tilgjengelig for inntrengere. E-postadressene dine kan brukes til å sende søppelpost, og informasjon i sosiale medier kan endres.

Det trådløse hjemmenettverket er også truet. For eksempel kan WPA2-protokollen hackes ved hjelp av et KRACK-angrep (Key Reinstallation Attack).

Du må alltid følge disse anbefalingene når du kobler til et hvilket som helst trådløst nettverk:

1. Kontroller at Brannmur er installert og slått på. Denne beskyttelseskomponenten skanner nettverkstrafikk og beskytter datamaskinen mot nettverksangrep.

2. Brannmur er en del av følgende Kaspersky-programmer: Kaspersky, Kaspersky Internet Security, Kaspersky Anti-Virus, Kaspersky Total Security, Kaspersky Security Cloud og Kaspersky Small Office Security.

3. Bruk en sikker HTTPS-tilkobling. Sørg for at adressefeltet i nettleseren din viser et grønt eller grått hengelåsikon.

4. Beskytt tilkoblingen med VPN. Installer Kaspersky Secure Connection på enheten, og aktiver en sikker tilkobling hver gang du kobler til Internett.

5. Hvis du bruker Windows, bør du deaktivere fil- og skriverdelingstjenesten for alle offentlige nettverk du kobler til. Se nettstedet til Microsoft Kundestøtte for instruksjoner.

6. Hvis du kan, bør du bruke mobildata i stedet for offentlige trådløse nettverk.

WPS er tilgjengelig på hjemmenettverket ditt

Formålet med WPS-teknologien er å gjøre det enklere å koble enheter til trådløse nettverk. WPS kan brukes til å koble til ruteren din uten et passord. Vi anbefaler å deaktivere WPS i ruterinnstillingene.

> Ruterens grensesnitt varierer avhengig av produsent, modell og fastvareversjon. Brukerhåndboken for rutermodellen din for å forstå innstillingene. Brukerhåndboken følger vanligvis med ruteren. Eventuelt kan du laste den ned fra nettstedet til enhetens produsent.

Følgende er et eksempel på konfigurasjonen for ruteren TP-Link TL-WR841N.

Slik deaktiverer du WPS:

1. Skriv inn IP-adressen til ruteren i adressefeltet i nettleseren din.

   Du kommer da til godkjenningssiden til webgrensesnittet for ruterkonfigurering. IP-adressen til ruteren er angitt på undersiden av enheten og i brukerhåndboken.

2. På godkjenningssiden skriver du inn brukernavnet og passordet ditt. Hvis du aldri endret disse, finner du dem på undersiden av ruteren.

3. På siden med ruterinnstillinger går du til delen **Trådløst** → **WPS**.

4. Klikk på **Deaktiver**.

Hjemmenettverket ditt er ikke passordbeskyttet

Uten passord er Wi-Fi-nettverket ditt tilgjengelig for alle. Et sterkt passord hindrer andre i å koble seg til nettverket ditt. Se denne artikkelen for anbefalinger om hvordan du oppretter et sterkt passord.

> Ruterens grensesnitt varierer avhengig av produsent, modell og fastvareversjon. Brukerhåndboken for rutermodellen din for å forstå innstillingene. Brukerhåndboken følger vanligvis med ruteren. Eventuelt kan du laste den ned fra nettstedet til enhetens produsent.

Følgende er et eksempel på konfigurasjonen for ruteren TP-Link TL-WR841N.

Slik oppretter du et passord:

1. Skriv inn IP-adressen til ruteren i adressefeltet i nettleseren din.

   Du kommer da til godkjenningssiden til webgrensesnittet for ruterkonfigurering. IP-adressen til ruteren er angitt på undersiden av enheten og i brukerhåndboken.

2. På godkjenningssiden skriver du inn brukernavnet og passordet ditt. Hvis du aldri endret disse, finner du dem på undersiden av ruteren.

3. På siden med ruterinnstillinger går du til delen **Trådløst** → **Trådløs sikkerhet**.

4. Velg **WPA/WPA2 – Personlig**.

5. I feltet **Trådløst passord** oppretter og angir du et Wi-Fi-passord.

6. Klikk på **Lagre**.

Hjemmenettverket ditt har en populær SSID

En teknikk som ofte brukes for å hacke passord, er den såkalte regnbuetabellen. Inntrengeren bruker en klargjort regnbuetabell med millioner av mulige passord for populære SSID-er. Hvis du har en SSID og et passord som finnes i en slik tabell, kan inntrengeren bruke spesiell programvare for å gjenopprette nettverkspassordet umiddelbart.

Bruk en sjelden SSID for å forbedre sikkerheten til det trådløse hjemmenettverket ditt.

> Ruterens grensesnitt varierer avhengig av produsent, modell og fastvareversjon. Brukerhåndboken for rutermodellen din for å forstå innstillingene. Brukerhåndboken følger vanligvis med ruteren. Eventuelt kan du laste den ned fra nettstedet til enhetens produsent.

Følgende er et eksempel på konfigurasjonen for ruteren TP-Link TL-WR841N.

Slik redigerer du navnet til det trådløse nettverket:

1. Skriv inn IP-adressen til ruteren i adressefeltet i nettleseren din.

   Du kommer da til godkjenningssiden til webgrensesnittet for ruterkonfigurering. IP-adressen til ruteren er angitt på undersiden av enheten og i brukerhåndboken.

2. På godkjenningssiden skriver du inn brukernavnet og passordet ditt. Hvis du aldri endret disse, finner du dem på undersiden av ruteren.

3. På siden med ruterinnstillinger går du til delen **Trådløst** → **Grunnleggende innstillinger**.

4. I feltet **Navn på trådløst nettverk** finner du på og skriver inn et navn for det trådløse nettverket ditt.

5. Klikk på **Lagre**.

Hjemmenettverket ditt bruker svak datakryptering

Når du bruker et nettverk med svak kryptering, kan inntrengere fange opp dataene dine. Hvis du får en melding om svak kryptering når du kobler til hjemmenettverket, bør du bytte til en sikrere krypteringstype. Trådløse nettverk bruker vanligvis følgende krypteringstyper: WEP, TKIP, WPA, WPA2 (AES/CCMP).

Den største forskjellen er beskyttelsesnivået de tilbyr. Vi anbefaler å bruke WPA2, fordi det er det sikreste alternativet.

Ruterens grensesnitt varierer avhengig av produsent, modell og fastvareversjon. Brukerhåndboken for rutermodellen din for å forstå innstillingene. Brukerhåndboken følger vanligvis med ruteren. Eventuelt kan du laste den ned fra nettstedet til enhetens produsent.

Følgende er et eksempel på konfigurasjonen for kryptering for ruteren TP-Link TL-WR841N.

Slik bruker du en annen krypteringstype for det trådløse nettverket ditt:

1. Skriv inn IP-adressen til ruteren i adressefeltet i nettleseren din.

   Du kommer da til godkjenningssiden til webgrensesnittet for ruterkonfigurering. IP-adressen til ruteren er angitt på undersiden av enheten og i brukerhåndboken.

2. På godkjenningssiden skriver du inn brukernavnet og passordet ditt. Hvis du aldri endret disse, finner du dem på undersiden av ruteren.

3. På siden med ruterinnstillinger går du til delen **Trådløst** → **Trådløs sikkerhet**.

4. Velg **WPA/WPA2 – Personlig**.

5. I feltet **Godkjenningstype** velger du **WPA2-PSK**.

6. I feltet **Kryptering** velger du **AES**.

7. Klikk på **Lagre**.

Hjemmenettverket ditt bruker et svakt passord

Vi anbefaler å bruke sterke passord for å beskytte personlige data og konfidensiell informasjon. Ikke opprett kontoer uten passord.

Sterke passordkrav

- Passordet må være minst åtte tegn langt. Hvis du bruker Windows, må du sørge for at minste passordlengde som er konfigurert i innstillingene for operativsystemet er minst åtte tegn.
- Passordet må inneholde store bokstaver, små bokstaver, tall, mellomrom og spesialtegn. For eksempel: oNQZnz$Hx2.

Passordet må ikke inneholde

- personopplysninger som andre enkelt kan få tak i. For eksempel for- eller etternavn, fødselsdato.
- Åpenbare og enkle ord, setninger, uttrykk og tegnsekvenser som er enkle å gjette seg til. For eksempel: passord, parol, abcd, qwerty eller asdfg, 1234567.

Teknikker for generering av passord

- Lag din egen algoritme for å komponere passord. Ta for eksempel favorittdiktet ditt, eller et kjent sitat. Skriv det ned med små og store bokstaver i det latinske alfabetet og erstatt noen av de med lignende tall og spesialtegn: @_R0s3 bY_a#y Ot#er n@mE w0u1c|_$me11 as_sVV3Et.
- Bruk en passordgenerator. Du kan bruke Kaspersky Password Manager til å generere komplekse passord, bekrefte passordenes styrke og lagre passordene sikkert. Du kan også installere leserutvidelsen for Kaspersky Password Manager for å fylle ut felter på nettsteder automatisk.

Hvor ofte bør jeg endre passordet mitt?

Vi anbefaler at du endrer passordet hver tredje måned.

Sikring av passordet

- Ikke avslør eller send passordet ditt til noen.
- Ikke la passordene dine være skrevet ned på et papirark på steder der andre kan se dem.
- Bruk et passordbehandlingsprogram eller passordlager som er innebygd i nettleseren din.
- Bruk et unikt passord for hver av kontoene dine. Hvis du bruker det samme passordet flere steder, kan en inntrenger som finner ut passordet til en av kontoene dine få tilgang til alle de andre kontoene dine.

Kategorien Alle programmer

Programlisten

Denne listen inneholder programmer som er installert på datamaskinen din. Du kan vise informasjon om status, digital signatur, klareringsgruppe, popularitet blant KSN-brukere og tidspunktet da det sist ble startet for hvert program på listen.

Dobbeltklikk på raden til et program eller en prosess for å åpne vinduet **Programregler**. I dette vinduet kan du konfigurere regler for å kontrollere programmets handlinger.

Høyreklikk på raden til programmet for å åpne hurtigmenyen. Fra hurtigmenyen kan du utføre følgende handlinger:

- Åpne vinduet **Programregler**, der du kan konfigurere tillatelser for programaktiviteter.
- Tillat eller blokker oppstart av program.
- Flytte programmet til en annen klareringsgruppe.
- Bruke standardinnstillinger for rettigheter i et program (tilbakestill programinnstillinger).
- Fjerne programmet fra listen.
- Åpne mappen som inneholder den kjørbare filen til programmet.

Programmer i listen inkluderes i grupper og undergrupper. Høyreklikk på raden til gruppen for å åpne hurtigmenyen. Fra hurtigmenyen kan du utføre følgende handlinger:

- Åpne vinduet **Grupperegler**, der du kan sette opp standardtillatelser for handlingene til programmer i denne gruppen.
- Opprett en undergruppe i gruppen. Som standard vil reglene som er spesifisert for gruppen en undergruppe tilhører brukes for denne undergruppen.
- Legg til et program i gruppen. Som standard vil reglene som er spesifisert for gruppen et program tilhører brukes for dette programmet.
- Bruk «Standardinnstillingene for rettigheter i et program» for gruppen og alle undergrupper og programmer i denne gruppen (tilbakestill gruppeinnstillinger).
- Bruk «Standardinnstillingene for rettigheter i et program» for alle undergrupper og programmer i gruppen, men ikke endre gruppens innstillinger (tilbakestill undergrupper og programinnstillinger).
- Slett undergrupper og programmer fra gruppen.

Program

Denne kolonnen viser programmets navn.

Status

Denne kolonnen viser programmets status: *Kjører* eller *Stoppet*.

Digital signatur

Denne kolonnen viser informasjon som angir om programmet har en digital signatur og hvem som eier denne signaturen.

Klareringsgruppe

Denne kolonnen viser klareringsgruppen som programmet tilhører. Klareringsgrupper definerer regler for bruk av programmet på datamaskinen: nekte eller tillate oppstart, programmets tilgang til filer og systemregisteret og restriksjoner for programmets nettverksaktivitet.

Popularitet

Denne kolonnen viser programmets popularitet blant deltakerne i Kaspersky Security Network (KSN). Popularitetsnivået avhenger av antallet KSN-deltakere som bruker programmet.

Siste kjøring

Denne kolonnen viser det siste tidspunktet da programmet ble startet.

Vinduet Grovt språk

Avtale

Den inneholder vilkårene som du må oppfylle for å gjøre endringer i listen over obskøne ord.

Jeg er voksen og godtar vilkårene

Ved å aktivere denne avmerkingsboksen godtar du vilkårene. Hvis boksen er avkrysset, er listen over obskøne uttrykk tilgjengelig for redigering.

Hvis boksen ikke er aktivert, er ikke listen over obskøne uttrykk tilgjengelig for redigering.

Programmer mikrofontilgang er blokkert for

Dette vinduet viser programmene du har blokkert mikrofontilgang for.

Tillat tilgang til mikrofon

Klikk på denne knappen for å gi programmet som er valgt i listen, tilgang til mikrofonen.

Vinduet Send tilbakemelding

Problem

En rullegardinliste der du kan velge en kategori for tilbakemeldingene dine. Tilbakemeldingskategorien kan vedrøre problemet med et nettsted åpnet i Beskyttet nettleser:

- **Jeg bruker det ikke**. Velg dette elementet hvis du ikke bruker Safe Money eller har besluttet å avvelge bruk av Safe Money.
- **Nettstedet åpnes for tregt**. Velg dette elementet hvis det tar lengre tid å åpne nettstedet enn det tar i en vanlig nettleser.
- **Beskyttet nettleser starter når det ikke trengs**. Velg dette elementet hvis nettsteder som ikke krever bruk av Safe Money, åpnes i Beskyttet nettleser.
- **Nettstedet kan ikke autoriseres**. Velg dette elementet hvis det oppstår feil under autorisasjonsforsøk på et nettsted åpnet i Beskyttet nettleser.
- **Nettstedet vises feil eller åpnes ikke**. Velg dette elementet hvis nettsteder ikke åpnes i Beskyttet nettleser eller vises med feil eller forvrengninger.
- **Feil ved verifisering av nettstedets sertifikat**. Velg dette elementet hvis feilmeldinger vises under valideringen av nettstedssertifikater.
- **Kunne ikke ta et skjermbilde mens Beskyttet nettleser kjører**. Velg dette elementet hvis skjermbilder ikke opprettes i Beskyttet nettleser.
- **Feil under inntasting eller innliming fra tastaturet eller utklippstavlen**. Velg dette elementet hvis det oppstår feil under inntasting av data i Beskyttet nettleser.
- **En nettside åpnet i Beskyttet nettleser kan ikke skrives ut**. Velg dette elementet hvis du ikke kan skrive ut en åpen side på et nettsted.
- **Det vises en melding som advarer om viktige operativsystemoppdateringer som ikke er installert**. Velg dette elementet hvis «Viktige systemoppdateringer er ikke installert» vises når du kjører Beskyttet nettleser.
- **En annen nettleser kjører som Beskyttet nettleser**. Velg dette elementet hvis Beskyttet nettleser åpnes i en annen nettleser enn den du starter den med.
- **Feil under bruk**. Velg dette elementet hvis du opplever feil med Beskyttet nettleser som ikke er på listen.
- **Annet**. Velg dette elementet hvis problemet du opplever ikke dekkes av andre elementer.

Du er ikke pålagt å spesifisere tilbakemeldingskategorien.

Detaljer

Du kan bruke dette feltet til å oppgi informasjon som kan hjelpe Kaspersky med å løse problemet. Dette feltet er valgfritt.

Send

Sende tilbakemeldingen til Kaspersky

Du kan sende tilbakemeldinger om operasjonen til komponenten Safe Money opptil ti ganger hver dag. Hvis programmet ikke kan sende tilbakemeldingen (for eksempel fordi du ikke har internettforbindelse), lagres tilbakemeldingen på datamaskinen. Den lagrede tilbakemeldingen vil være synlig i 30 dager.

Om et barns bruk av programmet

Hvis Kaspersky Safe Kids er installert og brukes på datamaskinen din, kan barnet bruke Kaspersky-programmet til å deaktivere Kaspersky Safe Kids. Hvis du vil unngå dette, anbefaler vi at du beskytter tilgang til innstillingene for Kaspersky med et passord.

Hvis du logget på operativsystemet med en konto som er koblet til en barneprofil i Kaspersky Safe Kids, vil Kaspersky slutte å vise følgende varslinger:

- Varslinger om sikkerhetsnyheter
- Varslinger om at det er oppdaget svake innstillinger i operativsystemet
- Varslinger om at den gjeldende enhetens kobles til et trådløst nettverk
- Varslinger om at en enhet kobles til et trådløst hjemmenettverk
- Nettleservarslinger om at et svakt passord angis på et nettsted
- Advarsler om at passordet du angir på et nettsted allerede har blitt brukt på et annet nettsted

Du kan aktivere varslinger ved å velge alternativet **Vis varslinger i barnas kontoer** i vinduet **Innstillinger** → **Grensesnitt**.

Tillatelser

Et passord beskytter følgende programinnstillinger mot å bli endret av en brukergruppe. Hvis en avkrysningsboks ved siden av en handling velges, betyr det at brukeren eller brukergruppen har tillatelse til å utføre den valgte handlingen.

Konfigurer programinnstillinger	Endre programinnstillinger i hovedvinduet, **Innstillinger**-vinduet, Varslingssenter og varsler. Aktivere og deaktivere programspor.
Styre sikkerhetskopiering og gjenoppretting	Opprette, endre og fjerne jobber for sikkerhetskopiering og gjenoppretting.
Administrer barns beskyttelse	Blokker oppstart av Kaspersky Safe Kids ved å bruke komponenten Inntrengningsbeskyttelse for verten, avslutt Kaspersky-programmet eller konfigurer Kaspersky-programmet for å deaktivere beskyttelsen. Når du prøver å laste ned, installere eller starte Kaspersky Safe Kids, kreves det ikke noe passord.
Avslutt programmet	Avslutt programmet.
Fjern/endre/gjennopprett	Fjerne/endre/gjenopprette programmet.
Fjern nøkkel	Fjerne eller endre en aktiveringskode og reserve-aktiveringskode.
Vis rapporter	Gå til **Rapporter**-vinduet.
Deaktivere beskyttelseskomponenter	Deaktiver og aktiver beskyttelseskomponenter i vinduet **Innstillinger**.

Feilsøking / Rull tilbake endringer

Dette vinduet viser fremdriften til reparasjon av skader i operativsystemet som ble oppdaget under analysen. Det kan ta litt tid å reparere skadene.

Hvis du valgte **Rull tilbake endringer** på første trinn, vil Feilsøkingsveiviseren i Microsoft Windows tilbakestille handlingene du valgte på forrige trinn.

Vinduet Abonnementsdetaljer

Dette vinduet viser følgende abonnementsinformasjon for programmet:

- Abonnementsstatus
- Antall dager igjen til abonnementet utløper
- Antall enheter som dekkes av abonnementet
- Aktiveringsdato
- Abonnementets utløpsdato

Slik konfigurerer du en VPN-tilkobling for et valgt nettsted

Slik konfigurerer du en VPN-tilkobling for et valgt nettsted:

1. Åpne hovedvinduet.
2. Åpne hovedvinduet og klikk på ☰-knappen.
3. Velg **Innstillinger** → **Nettsteder**.
4. Klikk på **Innstillinger**-knappen.

   Vinduet **Regler for tilkobling til nettsteder** vil da åpne.
5. I blokken **Unntak for nettsteder** klikker du på **Innstillinger**-knappen.

   Vinduet **Unntak for nettsteder** vil da åpne.
6. Klikk på **Legg til** for å legge til et nettsted i listen med unntak fra innstillingene som er spesifisert for nettstedkategorier.

   Vinduet **Legg til nettsted** vil da åpne.
7. Skriv inn nettadressen i feltet **Nettadresse (URL)**.
8. Under **Handling som skal utføres ved tilgang til nettstedet** spesifiserer du hvilken handling programmet skal utføre når du besøker dette nettstedet:

   - **Aktiver VPN**. Programmet aktiverer VPN når du besøker det spesifiserte nettstedet. Du kan for eksempel konfigurere programmet til å aktivere VPN når du besøker nettstedet til banken din. Denne innstillingen brukes selv om alternativet **Ignorer** er valgt i delen **Når du bruker de usikre nettstedene til banker** i vinduet **Regler for tilkobling til nettsteder**.

     a. I rullegardinmenyen **Velg den virtuelle serveren** velger du området og byen hvor du vil opprette en VPN-tilkobling, når du besøker dette nettstedet. Hvis området som er valgt for VPN for nettstedet ikke er det samme som området eller byen som er valgt for nettstedkategorien nettstedet tilhører, opprettes tilkoblingen til nettstedet gjennom området eller byen som er angitt for dette nettstedet, og ikke gjennom området for nettstedkategorien.

     b. Velg alternativet **Varsle hvis aktivert** hvis du ønsker å motta varslinger om at VPN aktiveres når du besøker dette nettstedet.

   - **Ignorer**. Programmet oppretter ikke VPN når du besøker det spesifiserte nettstedet.
9. Klikk på **Legg til**.

Programmet aktiverer ikke VPN hvis HTTPS-protokollen brukes til å koble til et nettsted.

Gå tilbake til hjelpen for Kaspersky VPN Secure Connection.

Slik konfigurerer du en VPN-tilkobling for nettstedkategorier

Som standard etablerer Kaspersky VPN ikke en sikker tilkobling når du åpner nettsteder i en nettleser. Du kan konfigurere aktivering av VPN for forskjellige nettstedkategorier hvis Kaspersky Plus eller Kaspersky Premium er installert og aktivert på datamaskinen din. Du kan for eksempel spesifisere at en VPN-tilkobling må etableres når du besøker nettstedene til betalingssystemer eller sosiale nettverk.

Slik konfigurerer du en VPN-tilkobling for nettstedkategorier:

1. Åpne hovedvinduet.
2. Åpne hovedvinduet og klikk på ☰-knappen.
3. Velg **Innstillinger** → **Nettsteder**.
4. Klikk på **Innstillinger**-knappen.

   Vinduet **Regler for tilkobling til nettsteder** vil da åpne.
5. Velg nettstedskategori:
   - Nettbanksider. Denne kategorien inkluderer bankers nettsteder.
   - Betalingssystemer. Denne kategorien inkluderer nettsteder for betalingssystemer.
   - Nettbutikker med betaling på nett. Denne kategorien inkluderer nettsteder for nettbutikker med innebygde betalingssystemer.
   - Sosiale nettverk. Denne kategorien inkluderer nettsteder for sosiale nettverk.
6. Velg en handling som utløses når denne nettstedskategorien besøkes:
   - **Aktiver VPN**. Programmet aktiverer VPN når du besøker nettsteder i denne kategorien.
   - **Spør**. Når du besøker et nettsted i denne kategorien, vil programmet spørre deg om det skal etableres en VPN for nettstedet. I nettleservinduet velger du den aktuelle handlingen og merker av for **Husk mitt valg for dette nettstedet**. Programmet vil utføre den valgte handlingen hver gang du besøker dette nettstedet. Hvis avkrysningsboksen ikke er valgt, husker programmet valget ditt i én time.
   - **Ignorer**. Programmet vil ikke aktivere en VPN når du besøker nettsteder i denne kategorien.
7. Hvis alternativet **Aktiver VPN** er aktivert, velger du rullegardinmenyen **Velg den virtuelle serveren** og angir området og byen du ønsker å opprette en VPN-tilkobling gjennom, for denne nettstedkategorien.
8. Velg alternativet **Varsle hvis aktivert** hvis du ønsker å motta varslinger om at en sikker tilkobling aktiveres når du besøker nettsteder i denne kategorien.

Kaspersky VPN Secure Connection vil som standard ikke aktivere en VPN-tilkobling hvis HTTPS-protokollen brukes til å koble til et nettsted.

Gå tilbake til hjelpen for Kaspersky VPN Secure Connection.

Inntrengningsbeskyttelse

Delen **Programmer** viser informasjon om antallet programmer som kontrolleres av Kaspersky.

Behandle programmer

Ved å klikke på denne lenken åpnes vinduet **Behandle programmer**. I dette vinduet kan du angi grupper med klarerte programmer, tillate og blokkere start av programmer og gå til konfigurasjon av tillatelser for et valgt program.

Delen **Gjeldende aktivitet** viser informasjon om antallet aktive programmer og prosesser. Informasjon om belastningen på harddisken, RAM-volum, ledig diskplass og nettverksaktiviteter vises i grafisk format.

Vis aktivitet

Klikk på denne koblingen for å åpne vinduet **Programaktivitet** med kategorien **Kjører** åpen. I dette vinduet kan du vise ressursbruken til hvert av de aktive programmene, eller du kan gå til konfigurasjon av tillatelser for et valgt program.

Unntak for Inntrengningsbeskyttelse

Unntak

Inneholder ressurser med personlige data som er utelukket fra beskyttelsesomfanget til Inntrengningsbeskyttelse. En ressurs kan være en fil, en mappe eller en registernøkkel.

Ressurs

Denne kolonnen viser ressursens navn.

Bane

Denne kolonnen viser hvor ressursen er lagret. Banen kan inneholde en maske.

Status

Denne kolonnen inneholder en rullegardinliste med alternativer for ressursstatus:

- **Aktiver kontroll**. Hvis dette alternativet er valgt, kontrollens aktiviteter som er spesifikke for denne ressursen.
- **Deaktiver kontroll**. Hvis dette alternativet er valgt, kontrolleres ikke aktiviteter som er spesifikke for denne ressursen.

Du kan aktivere eller deaktivere ressurskontroll i rullegardinlisten ved å venstreklikke på statusikonet.

Legg til

Klikk på denne knappen for å åpne et vindu der du kan angi ressursen med personlige data du vil legge til i listen.

Rediger

Klikk på denne knappen for å åpne vinduet **Rediger fil eller mappe** / **Rediger registernøkkel**. I dette vinduet kan du redigere innstillingene til ressursen.

Du kan ikke redigere ressurser som er lagt til i listen som standard.

Slett

Klikk på denne knappen for å fjerne den valgte ressursen fra Programlisten.

Du kan ikke slette ressurser som er lagt til i listen som standard.

Kategorien Generelt

Kategorien Generelt

Beskrivelse av den valgte gruppen med programmer.

Kategorien Ressurser

I denne kategorien kan du velge system- og brukerressurser og definere programmers tilgang til disse ressursene ved å endre rettighetene.

Knappen 

Med denne knappen kan du vise eller skjule panelet for regelinnstillinger.

Vis

Fra denne rullegardinlisten kan du velge to alternativer for filtrering av ressurser:

- **Skjul systemprogrammer**. Hvis du velger dette alternativet, skjules ressursene til systemprogrammer i listen over ressurser.
- **Skjul <PRODUCT>**. Hvis du velger dette alternativet, er ressursene til Kaspersky skjult i listen.

Operativsystem

Denne listen inneholder innstillinger for ressurser for operativsystemet i den valgte kategorien. En ressurs kan være en fil, en mappe, registernøkkel, nettverkstjeneste eller IP-adresse. Inntrengningsbeskyttelse overvåker andre programmers tilgang til ressursene på listen.

Som standard inneholder listen **Operativsystem** følgende objekter:

- Registernøkler som inneholder oppstartsinnstillinger
- Registernøkler som inneholder innstillinger for Internett-bruk
- Registernøkler som påvirker sikkerheten til operativsystemet
- Registernøkler som inneholder systemserviceinnstillinger
- Systemfiler og mapper
- Oppstartsmapper

Personlige data

Inneholder brukerens personlige data, fordelt etter ressurser og kategorier. En ressurs kan være en fil eller en mappe. Inntrengningsbeskyttelse analyserer handlingene som andre programmer utfører på de oppførte ressursene.

Som standard inneholder personopplysningslisten følgende objekter:

- Brukerfiler (mappen Mine dokumenter, informasjonskapselfiler, informasjon om brukerens aktivitet)
- Filer, mapper og registernøkler som inneholder innstillinger og viktige data for programmene som brukes oftest: nettlesere, filbehandlere, e-postklienter, direktemeldingsklienter og elektroniske lommebøker.

Ressurs

Denne kolonnen viser navnet på operativsystemressursen som er beskyttet av Inntrengningsbeskyttelse.

Bane

Denne kolonnen viser hvor ressursen er lagret. Banen kan inneholde en maske.

Status

Denne kolonnen inneholder en rullegardinliste med alternativer for ressursstatus:

- **Aktiver kontroll**. Hvis dette alternativet er valgt, kontrollens aktiviteter som er spesifikke for denne ressursen.
- **Deaktiver kontroll**. Hvis dette alternativet er valgt, kontrolleres ikke aktiviteter som er spesifikke for denne ressursen.

Du kan aktivere eller deaktivere ressurskontroll i rullegardinlisten ved å venstreklikke på statusikonet.

Legg til

I denne rullegardinlisten kan du legge til en ressurskategori, fil eller mappe med ressurser, eller en systemregisternøkkel.

Rediger

Når du klikker på denne koblingen, åpnes et vindu der du kan redigere navnet på og banen til den valgte ressursen.

Slett

Klikk på denne koblingen for å fjerne den valgte ressurskategorien, filen eller mappen med ressurser eller en systemregisternøkkel fra listen. Inntrengningsbeskyttelse vil slutte å kontrollere andre programmers tilgang til denne ressursen.

Gjenopprett

Du kan velge en av følgende alternativer fra denne rullegardinlisten:

- **innstillinger for kategori**. Hvis dette alternativet er valgt, tilordnes standardverdier til innstillingene for den valgte kategorien.
- **innstillinger for undergrupper og ressurser**. Hvis dette alternativet er valgt, tilordnes standardverdier til undergrupper og ressurser som tilhører den valgte kategorien.

Programlisten

Denne listen viser klareringsgrupper og programmer som tilhører disse gruppene. Kolonnene **Les**, **Skriv**, **Opprett** og **Slett** angir tilgangsrettighetene til et program eller en gruppe med programmer for den valgte ressursen.

I tabellen nedenfor finner du en liste over handlingene som skal utføres av Kaspersky når et program eller en programgruppe prøver å få tilgang til ressursen.

Beskrivelse av handlingene til Kaspersky

Handling	Beskrivelse
Arv	Programmet eller gruppen arver responsen fra den overordnede gruppen.
Tillat	Kaspersky tillater at programmene i den valgte gruppen får tilgang til ressursen.
Nekt	Kaspersky blokkerer tilgang til ressursen for programmene i den valgte gruppen.
Spør brukeren	Hvis alternativet **Utfør anbefalte handlinger automatisk** er aktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**, velger Kaspersky handlingen som skal utføres på denne ressursen automatisk basert på regler opprettet av Kasperskys eksperter. Du kan sjekke fotnoten for å lese nøyaktig hvilken handling som blir valgt. Hvis alternativet er deaktivert, vil Kaspersky spørre brukeren hvorvidt dette programmet skal tillates å få tilgang til ressursen.
Logg hendelser	Kaspersky registrerer ikke bare den angitte responsen i en rapport, men også informasjon om programmets forsøk på å få tilgang til ressursen.

Vinduet Lisensavtale for sluttbrukere

Vinduet inneholder teksten i lisensavtalen for sluttbrukere. Bruk rullefeltet til å vise lisensavtalen for sluttbrukere

Vinduet Lisensiering

Abonnementsdetaljer vises i delen øverst i vinduet:

- Abonnementsstatus
- Antall dager igjen til abonnementet utløper

Om lisensen din / Om abonnementet ditt

Klikk på denne koblingen for å åpne et vindu, som inneholder informasjon om det nåværende abonnementet.

Gå til My Kaspersky

Når du klikker på denne knappen, åpnes siden for My Kaspersky i den standard nettleseren.

Lisensavtale for sluttbrukere

Klikk på denne knappen for å åpne vinduet for å lese teksten i lisensavtalen.

Avhengig av abonnementet og egenskapene til den gjeldene programversjonen, vil vinduet vise ulike knapper for å starte handlinger knyttet til abonnementet. Standardknappene er beskrevet under.

Forny abonnement

Når du klikker på denne knappen, åpnes websiden til en nettbutikk, der du kan kjøpe et abonnement.

Knappen blir synlig dersom abonnementet er utløpt eller er i ferd med å utløpe.

Kjøp abonnement

Når du klikker på denne knappen, åpnes websiden til en nettbutikk, der du kan kjøpe et abonnement.

Denne knappen er tilgjengelig hvis abonnementet er blokkert eller prøveversjonen er utløpt.

Oppdater databaser

Klikk på denne knappen for å starte oppdatering av programdatabasene.

Knappen er tilgjengelig dersom problemene med den gjeldende lisensen kan løses ved oppdatering av databasene (for eksempel når utgivelsesdatoen for databasene ikke samsvarer med utløpsdatoen for lisensen).

Årsaker og mulige løsninger

Klikk på denne knappen for å åpne et nettleservindu med nettstedet for teknisk støtte, der du finner informasjon om det aktuelle problemet.

Denne knappen er tilgjengelig hvis det oppstår problemer med det gjeldende abonnementet.

Oppdater status

Klikk på denne knappen for å laste ned oppdatert informasjon om abonnementsstatus fra leverandørens server.

Denne knappen vises hvis programmet brukes med et abonnement.

Andre inkompatible programmer oppdaget

Listen over inkompatible programmer

Listen inneholder programmer som ikke er kompatible med programmet som blir installert. Fjern inkompatible programmer for forsvarlig drift av programmet som blir installert.

Fjern manuelt

Klikk på denne knappen for å åpne et vindu med en liste over programmer som er installert på datamaskinen. I denne listen kan du velge programmer som er inkompatible med programmet som installeres, for å fjerne dem fra datamaskinen.

Fortsett

Når du klikker på denne knappen, beholdes de oppførte, inkompatible programmene på datamaskinen og veiviseren fortsetter.

Samtidig bruk av inkompatible programmer og programmet som blir installert, kan føre til feil bruk av programmet du installerer og svekke beskyttelsen av datamaskinen betydelig.

Fant inkompatibel programvare

Listen over inkompatible programmer

Listen inneholder programmer som ikke er kompatible med programmet som blir installert. Fjern inkompatible programmer for forsvarlig drift av programmet som blir installert.

Slett

Når du klikker på denne knappen, fjernes de oppførte, inkompatible programmene fra datamaskinen og veiviseren fortsetter.

Behold

Når du klikker på denne knappen, beholdes de oppførte, inkompatible programmene på datamaskinen og veiviseren fortsetter.

Samtidig bruk av inkompatible programmer og programmet som blir installert, kan føre til feil bruk av programmet du installerer og svekke beskyttelsen av datamaskinen betydelig.

Omstart av datamaskinen kreves

Start datamaskinen på nytt

Dette alternativet aktiverer/deaktiverer omstart av datamaskinen. Datamaskinen må startes på nytt for at migrasjonsveiviseren skal fortsette.

Dersom boksen er avkrysset, kan du klikke på knappen **Fullført** for å starte maskinen på nyt, mens Veiviseren for migrering skal fortsette å kjøre.

Hvis alternativet er deaktivert, vil ikke datamaskinen startes på nytt. Migrasjonsveiviseren gjenopptas når du starter datamaskinen på nytt eller slår av og på datamaskinen.

Komme i gang

Vis sertifikatopplysninger

Kobling som åpner et vindu med informasjon om Kaspersky-sertifikatet.

Neste

Denne knappen starter veiviseren for installasjon av sertifikat.

Installasjon av sertifikat

Dette vinduet viser fremgangen i automatisk installasjon av sertifikatet. Det kan ta litt tid å fullføre oppgaven.

Kaspersky søker etter nettlesere som er installert på brukerens datamaskin, og installerer deretter automatisk sertifikater i Microsoft Windows sertifikatlager.

Når du installerer sertifikatet, vil du eventuelt se en sikkerhetsmelding fra Microsoft Windows, som ber deg om å bekrefte installasjonen av sertifikatet.

Fullføring av veiviseren

Fullført

Når du klikker på denne knappen, lukker Kaspersky veiviseren for installasjon av sertifikat.

Delen Blokkerte datamaskiner

Blokkerte datamaskiner

Inneholder informasjon om datamaskinene der Nettverkangrepsblokkering har forbudt all nettverksaktivitet rettet mot datamaskinen din.

Datamaskinadresse

Denne kolonnen viser IP-adressen til en blokkert datamaskin.

Tidspunktet da blokkeringen startet

Denne kolonnen viser tiden som har gått etter at datamaskinen ble blokkert.

Som standard blokkerer Nettverkangrepsblokkering innkommende trafikk i en time fra en datamaskin som angriper.

Hvis du vil oppheve blokkeringen for en datamaskin valgt i listen, må du åpne hurtigmenyen til datamaskinen.

Fjern blokkering

Når du klikker på denne knappen, vil Nettverkangrepsblokkering oppheve blokkeringen av den valgte datamaskinen.

Fjern blokkering av alle datamaskiner

Når du klikker på denne koblingen, opphever Nettverkangrepsblokkering blokkeringen for alle blokkerte datamaskiner.

Delen Åpne porter

Vis

Denne knappen åpner en meny som har følgende menyelementer:

- **Vis alle porter** – listen viser alle åpne porter på datamaskinen.
- **Skjul loopback-porter** – listen viser alle porter, unntatt de som brukes av nettverksprogramvaren i operativsystemet.

Åpne porter

Inneholder informasjon om alle åpne porter for hver prosess.

Følgende informasjon vises for hver port:

- Portnummer
- Navnet på prosessen (program, tjeneste, server) som bruker porten
- Prosess-ID
- Prosessens lokale IP-adresse
- Protokollen for tilkobling via porten

Når du dobbeltklikker på en linje på listen, åpnes vinduet **Programregler** med kategorien **Nettverksregler**. I dette vinduet kan du konfigurere nettverksregler for programmet som bruker den valgte porten.

Hvis du høyreklikker et element i listen, åpnes en hurtigmeny der du kan konfigurere nettverksregler.

Menyen har følgende menyvalg:

- **Programnettverksregler**. Dette menyelementet åpner vinduet **Programregler** i kategorien **Nettverksregler**. I dette vinduet kan du konfigurere en nettverksregel for et program som bruker porten som er valgt på listen.
- **Alle nettverksregler**. Hvis du velger dette menyelementet, åpnes vinduet **Pakkeregler**. I dette vinduet kan du konfigurere pakkeregler for et program som bruker porten som er valgt på listen.

Delen Nettverksaktivitet

Vis

Denne knappen åpner en meny. Menyen har følgende menyvalg:

- **Vis lokale tilkoblinger** – listen viser informasjon om tilkoblinger til andre datamaskiner i det samme lokale nettverket.
- **Vis tilkoblinger for <PRODUCT>** – listen viser informasjon om tilkoblingene som er opprettet av Kaspersky.

Nettverksaktivitet

Denne listen inneholder alle aktive nettverkstilkoblinger som er opprettet på datamaskinen.

Følgende informasjon for hver tilkobling vises:

- Navn på prosessen (program, tjeneste, server) som opprettet tilkoblingen
- Tilkoblingens retning (innkommende/utgående)
- Tilkoblingsprotokoll
- Tilkoblingsinnstillinger (ekstern port og IP-adresse)
- Størrelsen på data som er overført/mottatt (i kilobyte)

Hvis du høyreklikker et element i listen, åpnes en hurtigmeny der du kan konfigurere nettverksregler.

Menyen har følgende menyvalg:

- **Programnettverksregler**. Dette menyelementet åpner vinduet **Programregler** i kategorien **Nettverksregler**. I dette vinduet kan du konfigurere en nettverksregelen for et program som er valgt på listen.
- **Alle nettverksregler**. Hvis du velger dette menyelementet, åpnes vinduet **Pakkeregler**. I dette vinduet kan du konfigurere pakkeregler for et program som er valgt på listen.

Blokker all nettverksaktivitet

Klikk på denne koblingen for å blokkere nettverksaktiviteten til alle prosesser.

Nederst i vinduet vises et diagram over nettverkstrafikken. Dette diagrammet viser mengden innkommende og utgående trafikk for en prosess på listen. Diagrammet viser mengden trafikk i sanntid. Mengden trafikk vises i kilobytes.

Spesielle hensyn når du legger til en regel for et nettverkskort

Når du oppretter en tillatelsesregel for et nettverkskort og/eller en regel med en spesifisert TTL, kan denne regelen komme i konflikt med en avslagsregel for programmer. Hvis et program for eksempel er i gruppen Høyt begrenset, vil det bli nektet nettverkstilgang selv om du opprettet en regel for å tillate pakker for nettverksadapteren (og for TTL).

Hvis du vil konfigurere en tillatelsesregel som skal fungere for alle programmer som prøver å koble til nettverket via dette nettverkskortet, må du opprette følgende regler i prioritetsrekkefølge fra høyeste prioritet til laveste prioritet (i den generelle listen over pakkeregler fastslås prioritet fra topp til bunn, fra høyeste prioritet til laveste prioritet).

1. Tillat regel for det valgte nettverkskortet.
2. Avvis regler for alle andre nettverkskort.
3. Tillat regel uten å spesifisere et nettverkskort.

Hvis du vil konfigurere en tillatelsesregel som skal fungere for et nettverkskort med TTL, må du opprette følgende regler i prioritetsrekkefølge fra høyeste prioritet til laveste prioritet:

1. Tillat regel for en bestemt TTL-verdi.
2. Nekt regel for en TTL-verdi lik 255.
3. Tillat regel uten å spesifisere en TTL-verdi.

Delen Nettverkstrafikk

Periode

Listen inneholder tidsintervaller der du kan se fordelingen av nettverkstrafikk.

Alternativer:

- **For dagen**. Denne listen viser data om nettverkstrafikk for i dag.
- **For i går**. Denne listen viser data om nettverkstrafikk for foregående dag.
- **For måneden**. Denne listen viser data om nettverkstrafikk for inneværende måned.
- **For året**. Denne listen viser data om nettverkstrafikk for inneværende år.

Nettverkstrafikk

Inneholder informasjon om alle innkommende og utgående forbindelser opprettet mellom din datamaskin og andre datamaskiner.

Innkommende og utgående trafikkmengde vises for hvert program (datamaskin, tjeneste, server, prosess).

Når du dobbeltklikker på et program på listen, åpnes vinduet **Programregler** med kategorien **Nettverksregler**. I dette vinduet kan du konfigurere nettverksregler for det valgte programmet.

Hvis du høyreklikker et element i listen, åpnes en hurtigmeny der du kan konfigurere nettverksregler.

Menyen har følgende menyvalg:

- **Programnettverksregler**. Hvis du velger dette menyelementet, åpnes vinduet **Programregler** i kategorien **Nettverksregler**, der du kan konfigurere en nettverksregel for det angitte programmet.
- **Alle nettverksregler**. Hvis du velger dette menyelementet, åpnes vinduet **Pakkeregler**, der du kan konfigurere pakkeregler for det angitte programmet.

Nederst i vinduet vises et diagram over tidsfordelingen av trafikk for det valgte programmet, for det spesifiserte tidsintervallet.

Avslutning av nettverkstilkoblinger

Hvis datamaskinen slås av eller beskyttelsen stanses midlertidig mens programmet overvåker aktive nettverkstilkoblinger, vises et varsel om at disse tilkoblingene avsluttes. Det er nødvendig for å avslutte programmet på riktig måte. Avslutningen skjer automatisk etter en periode på 10 sekunder, eller når du klikker på **Ja**. De fleste avsluttede tilkoblinger gjenopprettes etter kort tid.

Hvis tilkoblingen avsluttes mens du laster ned en fil uten å bruke et nedlastingsprogram, avbrytes overføring av data. Du må starte nedlastingsprosessen på nytt for å laste ned filen.

Du kan avbryte avslutning av tilkoblinger. Det gjør du ved å klikke på **Nei**-knappen i varslingsboksen. Programmet vil fortsette å kjøre.

Om avanserte alternativer for VPN

Ytterligere funksjoner i VPN er tilgjengelige hvis Kaspersky Plus eller Kaspersky Premium er installert på datamaskinen din.

Tilleggsfunksjoner for VPN inkluderer:

- Innstillinger for aktivering av en VPN når følgende nettstedkategorier besøkes:
  - Nettbanker;
  - Betalingssystemer;
  - Nettbutikker og nettsteder for elektronisk handel;
  - Sosiale nettverk.
- Innstillinger for automatisk endring av område og by. Hvis du angir ulike områder og byer for nettstedkategorier i innstillingene for VPN, kan du spesifisere om du vil bytte område og by når du bytter mellom nettsteder i ulike kategorier.
- Innstillinger for VPN for enkelte nettsteder, for eksempel nettsteder du besøker ofte.

Gå tilbake til hjelpen for Kaspersky VPN Secure Connection.

Oppdagede objekter

Løs

Når du klikker på denne knappen, begynner Kaspersky-programmet å behandle det registrerte objektet.

Knappen er tilgjengelig dersom det er oppdaget et objekt.

Klikk på -knappen for å åpne en meny der du kan velge en annen handling:

- **Legg til i unntak** oppretter et unntak som definerer når objektet ikke skal ansees som skadelig.
- **Ignorer** flytter varslingen til delen **Ignorerte varsler**.
- **Åpne overordnet mappe** åpner mappen der filen opprinnelig var lagret.
- **Finn ut mer** åpner en webside med en beskrivelse av det oppdagede objektet.

Varslingsvinduer i Kaspersky

Meldinger som vises i systemstatusfeltet, informerer deg om programhendelser som krever din oppmerksomhet.

Hvis du ser en varsling på skjermen, bør du velge en av de anbefalte handlingene i varslingen. Det beste valget det som er anbefales som standard av Kasperskys eksperter.

Om skybeskyttelse

Du finner mer informasjon om Kaspersky Security Network i dette vinduet.

Vinduet Aktivering

Dette vinduet viser fremdriften til programaktiveringen.

Avbryt

Klikk på denne knappen for å avbryte aktivering av programmet.

Registrering og autorisering

E-postadresse

I dette feltet kan du angi en e-postadresse for å koble til en eksisterende My Kaspersky-konto eller opprette en ny konto.

Logg på med Google

Når du klikker på denne knappen, omdirigeres du til påloggingsskjemaet for Google-kontoen i standardnettleseren din (ikke tilgjengelig i noen områder).

Logg på med Facebook

Når du klikker på denne knappen, omdirigeres du til påloggingsskjemaet for Facebook-kontoen i standardnettleseren din (ikke tilgjengelig i noen områder).

Logg på med Apple

Når du klikker på denne knappen, omdirigeres du til påloggingsskjemaet for Apple-kontoen i standardnettleseren din.

Jeg har en aktiveringskode

Når du klikker på denne lenken, omdirigeres du til skjemaet for inntasting av aktiveringskode.

Fortsett

Når du klikker på denne knappen, omdirigeres du til skjemaet der du kan skrive inn passordet til en eksisterende My Kaspersky-konto, eller starte prosessen med å opprette en ny konto.

Når du logger på en eksisterende My Kaspersky-konto, viser vinduet følgende:

Passord

Skriv inn passordet for My Kaspersky-kontoen din i dette feltet.

Glemt passordet?

Bytt til dette vinduet for å gjenopprette et glemt passord for My Kaspersky-kontoen din.

Skriv inn en annen e-postadresse

Når du klikker på denne knappen, kommer du tilbake til skjemaet der du kan skrive inn e-postadresse.

Logg på

Klikk på denne knappen for å koble enheten til My Kaspersky-kontoen din.

Når du oppretter en My Kaspersky-konto, viser vinduet følgende:

Jeg godtar å gi Kaspersky e-postadressen min for å motta persontilpassede markedsføringstilbud

Hvis alternativet er aktivert, vil du motta nyheter fra Kaspersky til den angitte e-postadressen.

Region

Klikk på denne koblingen for å åpne vinduet for valg av område. Programmene du kan installere og de tilgjengelige betalingsmetodene som du kan bruke, avhenger av det valgte området.

Skriv inn en annen e-postadresse

Når du klikker på denne knappen, kommer du tilbake til skjemaet der du kan skrive inn e-postadresse.

Opprett

Når du klikker på denne knappen, registreres kontoen på My Kaspersky. Du vil motta en melding til e-postadressen du spesifiserte, med lenken for oppretting av passord.

Mer om My Kaspersky-kontoen

Vinduet Velg nøkkel fra registeret

Velg

Når du klikker på denne knappen, fylles feltene i vinduet **Legg til registernøkkel** ut med verdiene til den valgte nøkkelen.

Vinduet Velg plassering for hemmelig hvelv

I dette vinduet kan du velge plasseringen til det hemmelige hvelvet du oppretter.

Velg

Ved å klikke på denne knappen kan du bekrefte at den angitte banen er riktig.

Vinduet Velg fil eller mappe

Velg

Når du klikker på denne knappen, vises banen til en fil eller mappe i feltet **Bane** i vinduet **Legg til fil eller mappe**.

Vinduet Klarer gruppe for ukjente programmer

Dette vinduet viser programmer som ikke kunne legges til i eksisterende grupper. Du kan velge en klareringsgruppe og klikke på **Lagre**. Programmer som ikke kunne legges til andre grupper, vil bli lagt til i gruppen du spesifiserte.

Som standard legges disse programmene til i gruppen **Lavt begrenset**.

Klareringsgruppen for programmer som startes før hovedvinduet i Kaspersky

I dette vinduet kan du velge en klareringsgruppe for ukjente programmer som startes før Kaspersky-programmet.

Liste over klareringsgrupper

Bruk denne listen til å angi klareringsgruppen der programmer skal startes før Kaspersky-programmet, skal tilordnes til. Nettverksaktivitetene til slike programmer begrenses i henhold til reglene for den valgte klareringsgruppen. Som standard begrenses nettverksaktivitetene til programmer som startes før Kaspersky-programmet, i henhold til reglene konfigurert av Kaspersky.

Velg klareringsgruppe automatisk

Hvis dette alternativet er valgt, vil Inntrengningsbeskyttelse legge programmer som startes for Kaspersky-programmet starter til en klareringsgruppe basert på regler opprettet av Kaspersky-eksperter.

Velg klareringsgruppe manuelt

Hvis dette alternativet er valgt, kan du velge en klareringsgruppe som der programmer som startes før Kaspersky-programmet starter, legges til.

Vinduet Legg til / rediger Privat surfing

Nettadressemaske

I dette feltet angir du IP-adressen eller nettadressen (URLen) til nettstedet du vil tillate sporing av nettaktiviteter på.

Vinduet Legge til / redigere kategori

Kategorinavn

I dette feltet kan du angi navnet på en kategori med ressurser. Tilgangen til denne kategorien med ressurser vil analyseres og kontrolleres av Inntrengningsbeskyttelse.

Vinduet Legg til / rediger registernøkkel

Velg

Klikk på denne knappen for å åpne vinduet **Velg nøkkel fra registeret**, der du kan velge en registreringsnøkkel du vil at komponenten Inntrengningsbeskyttelse skal styre tilgangen til.

Navn

Du angir navnet på en ressurs med registernøkkelen i dette feltet.

Bane til nøkkel

Du angir banen til en registernøkkel i dette feltet.

Beskytt nøkkelverdi

Hvis dette alternativet er aktivert, beskyttes bare nøkkelverdien som er angitt i feltet **Nøkkelverdi** mot endringer.

Hvis alternativet er deaktivert, beskyttes alle verdiene til denne registernøkkelen.

Hvis ingen verdi er angitt i feltet **Nøkkelverdi**, beskyttes standardverdien til registernøkkelen som standard.

Dette alternativet aktiveres automatisk når du velger en registernøkkel.

Nøkkelverdi

I dette feltet kan du spesifisere verdien til en registernøkkel som må beskyttes mot endringer av komponenten Inntrengningsbeskyttelse.

Dette feltet kan kun redigeres hvis det er merket av for **Beskytt nøkkelverdi**.

Legg til

Klikk på denne knappen for å legge til en registernøkkel i listen over ressurser.

Vinduet Legg til / rediger upassende ord

Maske for uanstendig ord

Ord eller ordmasker som anses å være tegn på spam hvis de oppdages i en melding.

Vektskoeffisient for uanstendig ord

En numerisk verdi som angir sannsynligheten for at en melding som inneholder et bestemt ord, er spam. En høy vektkoeffisient angir stor sannsynlighet for at meldingen som inneholder det bestemte ordet, er spam.

Anti-Spam klassifiserer en melding som spam hvis totalsummen av vektkoeffisientene til de bestemte ordene og blokkerte uttrykkene i meldingen overgår den angitte grenseverdien.

Status

I delen **Status** kan du spesifisere hvorvidt Anti-Spam skal skanne meldinger for et bestemt ord:

- **Aktiv**. Anti-Spam skanner meldinger for å se om de inneholder et bestemt ord.
- **Inaktiv**. Anti-Spam skanner ikke meldinger for å se om de inneholder et bestemt ord.

Vinduet Legg til / rediger fil eller mappe

Navn

I dette feltet kan du spesifisere navnet til en ressurs med filen eller mappen du vil at tilgang til skal styres av Inntrengningsbeskyttelse.

Bane

I dette feltet kan du angi banen til en fil eller mappe manuelt.

Du kan bruke en maske når du angir banen manuelt.

Masken `\*` gjør at du kan spesifisere at du vil kontrollere tilgang til alle filer eller undermapper i den valgte mappen.

Masken `\*<extension>` gjør at du kan spesifisere at du vil kontrollere tilgang til alle filer med den spesifiserte utvidelsen i den valgte mappen.

Du kan også kontrollere programmenes tilgang til filressurser på en ekstern datamaskin. Det gjør du ved å angi banen til nettverksressursen i UNC-format i henhold til regelen `\\Server\Share\Relative path`, der:

- Server er domenenavnet til datamaskinen eller IP-adressen i IPv4- eller IPv6-format (påkrevd).
- Delt ressurs er nettverksnavnet til den delte mappen (påkrevd).
- Relativ bane er banen til mappen eller filen fra en delt mappe (valgfritt).

  Eksempler på baner:

- `\\Server1\ShareFolder1\test\example.exe`
- `\\Server1\ShareFolder1\test\*.docx`
- `\\Server1\ShareFolder1\*`

  Programmet kontrollerer ikke tilgang til filressursen hvis banen som er definert i regelen, er forskjellig fra den forespurte banen.

Velg

Klikk på denne knappen for å åpne et vindu der du kan velge en fil eller mappe.

Legg til

Klikk på denne knappen for å legge til en fil eller mappe i listen over ressurser.

Vinduet Aktivering fullført

Dette vinduet åpnes hvis programmet ble aktivert.

Fullført

Klikk på denne knappen for å fullføre programaktiveringen og åpne vinduet for lisensiering.

Vinduet Blokkerte og tillatte programmer

Dette vinduet viser en liste over programmer som har lov til eller ikke lov til å endre operativsysteminnstillinger. En tom liste betyr at du enda ikke har tillatt eller blokkert programmer fra å endre innstillingene i operativsystemet.

Programlisten

Programlisten inneholder følgende data:

- **Program**. Denne kolonnen viser programmets navn.
- **Filnavn**. Denne kolonnen viser navnet på den kjørbare filen til et program.
- **Bane**. Denne kolonnen viser banen til den kjørbare filen til et program på harddisken på datamaskinen din.
- **Leverandør**. Denne kolonnen viser den digitale signaturen til programutgiveren.
- **Endringer**. Denne kolonnen viser om et program er blokkert fra å endre eller har tillatelse til å endre innstillingene for operativsystemet, nettlesere og nettverk.

Vinduet Beskyttelse av personvern

I dette vinduet kan du aktivere og deaktivere følgende komponenter:

Webkamera og mikrofonkontroll

Datalekkasjekontroll

Privat surfing

Programoppdatering. Unntak

Unntak

Utelatte oppdateringer for installerte programmer legges inn i listen **Unntak**. Du kan hoppe over individuelle oppdateringer eller alle oppdateringer for et bestemt program installert på datamaskinen.

Listen **Unntak** inneholder følgende kolonner:

- **Program** – denne kolonnen viser programmets navn.
- **Hopp over** – denne kolonnen kan inneholde følgende verdier:
  - **Oppdateringens versjon** – dette vises hvis du hopper over en oppdatering for et installert program.
  - **Alle oppdateringer** – dette vises hvis du bestemte deg for å ikke oppdatere programmet.

Slett

Klikk på denne knappen for å fjerne de valgte programmene fra unntakslisten. Knappen er tilgjengelig hvis programmet er valgt i listen.

Kaspersky vil varsle deg om at det finnes oppdateringer for programmer som har blitt fjernet fra listen.

Vinduet Unntak for Privat surfing

Liste over unntak

Denne listen inneholder adressene til nettsteder der sporing av nettaktivitetene dine er tillatt. Privat surfing oppdager forsøk på datainnsamling på disse nettstedene, men blokkerer dem ikke, selv om komponenten er konfigurert til å blokkere datainnsamling fra disse kategoriene med sporingstjenester.

Du kan legge til en nettadresse eller en adressemaske på listen.

Rediger

Denne koblingen åpner et vindu der du kan endre den valgte nettadressen/adressemasken.

Slett

Fjerner den valgte nettadressen/adressemasken fra listen

Legg til

Denne koblingen åpner et vindu der du kan legge til en nettadresse/adressemaske.

Vinduet Programbruk

Programmer

Denne kolonnen viser programmer og programgruppe du kan begrense bruken av.

Bruk

Denne kolonnen viser hvorvidt brukeren tillates å bruke et program eller programgruppe:

- **Tillatt** – brukeren kan bruke dette programmet eller en programgruppe.
- **Blokkert** – brukeren tillates ikke å bruke dette programmet eller en programgruppe.
- **Begrenset** – brukeren kan bruke dette programmet eller en programgruppe i en begrenset tidsperiode.

Du kan tillate, blokkere eller begrense bruk av et program eller en programgruppe for den valgte brukeren, ved å velge ønsket element fra rullegardinlisten.

Bane

Denne kolonnen viser banen til programmets kjørbare fil.

Regler

Klikk på denne knappen for å åpne et vindu der du kan begrense hvor lenge det valgte programmet kan brukes.

Slett

Klikk på denne knappen for å slette det valgte programmet fra listen. Etter at programmet er fjernet fra listen vil Kaspersky slutte å overvåke bruken av programmet, og brukeren kan bruke dette programmet uten begrensninger.

Legg til program

Klikk på denne knappen for å åpne en dialogboks der du kan velge den kjørbare filen til et program og legge den til i listen. Foreldrekontroll legger til programmet i den tilsvarende kategorien i listen.

Vinduet Karantene

Objekter i Karantenelisten

Inneholder en liste over filer som er flyttet til Karantene. Karantene er beregnet på lagring av sikkerhetskopier av filer som er slettet eller endret under desinfiseringsprosedyren.

Fil

Denne kolonnen viser navnet på en fil i karantene.

Høyreklikk for å åpne en hurtigmeny der du kan velge handlinger for filer i karantene: gjenopprette, fjerne eller åpne i opprinnelig mappe.

Bane

Denne kolonnen viser banen til filen.

Detektert

Denne kolonnen viser den registrerte objekttypen, for eksempel *Nettverkangrep*.

Dato og klokkeslett

Denne kolonnen viser datoen og klokkeslettet da filen ble flyttet til Karantene.

Gjenopprett

Klikk på denne knappen hvis du vil at Kaspersky skal returnere en fil du har valgt i listen, til mappen den var lagret i før den ble flytte til Karantene.

Slett

Når du klikker på denne knappen, sletter Kaspersky filen som er valgt i listen.

Fjern alle

Når du klikker på denne knappen, vil Kaspersky slette alle sikkerhetskopier av filer som har blitt flyttet til Karantene.

Kaspersky desinfiserer ikke programmer i Windows Store. Hvis skanningsresultatene viser at en slik app er farlig, blir den slettet fra datamaskinen. Når en app i Windows Store blir slettet, oppretter ikke Kaspersky en sikkerhetskopi av den. Hvis du vil gjenopprette disse objektene, må du bruke gjenopprettingsverktøyene til operativsystemet (se dokumentasjonen til operativsystemet som er installert på datamaskinen, for mer informasjon) eller oppdater programmet fra Windows Store.

Vinduet Grovt språk

Dette vinduet viser en liste med grovt språk. Hvis Kaspersky finner noen av disse ordene i en melding, vil meldingen bli merket som spam.

Knappen

Klikk på denne knappen for å åpne en meny der du kan velge følgende handlinger:

- Importer og legg til i eksisterende. Velg dette alternativet hvis du vil importere en liste over obskøne uttrykk fra en CSV-fil. De aktuelle uttrykkene slettes ikke.
- Importer og erstatt eksisterende. Velg dette alternativet hvis du vil importere en liste over obskøne uttrykk fra en CSV-fil. De aktuelle uttrykkene slettes.
- Eksporter. Velg dette alternativet hvis du vil eksportere en liste over obskøne uttrykk til en CSV-fil.

Grovt språk

Denne kolonnen viser ordet eller uttrykket. At dette ordet eller uttrykket finnes i meldingen kan tyde på at den er spam.

Vekting

Kolonnen viser vektkoeffisienten som er tilordnet et grovt ord. Hvis en melding inneholder flere grove ord, og den kombinerte vektkoeffisienten av disse ordene overskrider 100, merkes denne meldingen som spam.

Status

Denne kolonnen viser om Anti-Spam bruker dette ordet under skanning etter grove ord i meldingene.

- **Aktiv**. Programmet søker etter dette ordet i meldinger.
- **Inaktiv**. Programmet søker ikke etter dette ordet i meldinger.

Rediger

Klikk på denne knappen for å åpne et vindu der du kan endre det bestemte ordet eller ordmasken som er valgt i listen.

Slett

Klikk på denne knappen for å slette et grovt ord.

Legg til

Når du klikker på denne knappen, åpnes et vindu der du kan legge til et ord eller en ordmaske i listen.

Vinduet Nyheter

Liste over nyheter

Nyheter vises som en liste i vinduet. Alle nyhetsoppføringer vises med tittel, annonsering og publiseringstidspunkt.

Klikk på denne knappen for å åpne vinduet med nyhetstekster.

Vinduet Nyheter

Koblinger til Twitter og sosiale nettverk

Klikk på disse koblingene for å åpne Twitter eller andre sosiale nettverk for å legge ut nyheter. Du kan redigere teksten som skal legges ut.

Hvis du ikke har logget på, åpnes påloggingssiden til det aktuelle sosiale nettverket.

Koblingene til sosiale nettverk vises hvis du har lov til å besøke disse webområdene.

Knappene

Knapper du kan klikke på for å veksle mellom nyhetsoppføringer.

Vinduet Innstillinger for Application Manager

Aktiver/deaktiver Application Manager

Aktiverer Application Manager. Hvis vekslebryteren er slått på, vil Kaspersky-programmet kontrollere installasjon og fjerning av tilleggsprogrammer og visning av installasjonstrinn som inneholder annonser.

Aktiverer Application Manager. Hvis vekslebryteren er slått på, vil Kaspersky-programmet kontrollere installasjon og fjerning av tilleggsprogrammer og visning av installasjonstrinn som inneholder annonser.

Deaktiver avmerkingsboksene for installasjon av tilleggsprogrammer når du installerer programmer. Advar mot alle forsøk på å installere tilleggsprogrammer

Hvis alternativet er aktivert, blokkerer Kaspersky-programmet installasjon av tilleggsprogrammer når du installerer programmer på datamaskinen.

Hvis alternativet ble deaktivert etter at du begynte å installere et bestemt program, fortsetter Blokkering av installasjon av uønskede programmer å kjøre under den nåværende installasjonen. Avmerkingsboksene ved siden av tilbud om installasjon av tilleggsprogrammer deaktiveres, og tilleggsprogrammene installeres ikke. Denne funksjonaliteten deaktiveres under neste installasjon. Ekstraprogrammer installeres sammen med hovedprogrammet.

Ikke vis installasjonstrinn som kan inneholde reklame og tilbyr å installere tilleggsprogrammer

Hvis alternativet er aktivert, vil Kaspersky blokkere visning av annonser og tilbud om å installere ekstra programvare når du installerer programmer på datamaskinen.

Innstillingsvinduet for Programoppdatering

Aktiver søk etter programoppdateringer

Hvis avkrysningsboksen er merket av, søker Kaspersky etter oppdateringer for installerte programmer og ber deg om å laste ned og installere dem.

Sett opp søkemodus for oppdateringer

Hvis du klikker på denne lenken, åpnes et vindu der du kan angi modusen for automatisk søk etter oppdateringer for programmer installert på datamaskinen.

Last ned og installer oppdateringer automatisk hvis du ikke må godta nye lisensavtaler

Hvis alternativet er valgt, søker Kaspersky-programmet etter oppdateringer for installerte programmer automatisk, for så å laste ned og installere de tilgjengelige oppgraderingene hvis dette ikke krever at du godtar nye lisensavtaler for sluttbrukere.

Søk etter programoppdateringer

I innstillingene må du velge hvilke programoppdateringer som må installeres:

- **Viktige oppdateringer som forbedrer datamaskinens sikkerhet** – betyr at det installeres kun viktige oppdateringer som reparerer sårbarheter i programvaren og forbedrer datamaskinens sikkerhet.
- **Alle oppdateringer for kjente programmer** betyr at alle oppdateringer installeres.

Unntak

Klikk på denne koblingen for å åpne vinduet **Unntak** med unntakslisten. Utelatte oppdateringer for installerte programmer legges inn i unntakslisten. Du kan hoppe over individuelle oppdateringer eller alle oppdateringer for et bestemt program installert på datamaskinen.

Søkemodus/tidsplan for oppdateringer

Tabellen beskriver innstillingene som kontrollerer planen for komponentene Programoppdatering og Application Manager.

Innstillinger	Beskrivelse
Oppdaterer søkemodus (Programoppdatering) **Kjør analyse** (Application Manager)	**Automatisk**. Kaspersky kjører oppgaven en gang hvert døgn i henhold til de interne innstillingene. **Hvert minutt** / **Hver time** / **Hver dag** / **Hver uke** / **Hver måned** / **På et bestemt tidspunkt**. Kaspersky kjører oppgaven i henhold til den definerte tidsplanen din, som kan spesifiseres til nærmeste minutt. Når et av disse alternativene er valgt, er listen **Utsett kjøring etter programoppstart for N minutter** tilgjengelig. **Etter at programmet har startet**. Når Kaspersky har startet, venter den i antall minutter som er angitt i feltet **Start om N minutter**, før den kjører oppgaven. **Etter hver oppdatering**. Kaspersky kjører oppgaven etter å ha lastet ned og installert en ny oppdateringspakke.
Søk etter oppdateringer neste dag hvis datamaskinen er slått av (Programoppdatering) **Kjør objektanalyse neste dag hvis datamaskinen er slått av** (Application Manager)	Hvis et planlagt søk etter programoppdateringer eller objektanalyser ble hoppet over fordi datamaskinen var slått av, kjører Kaspersky oppgaven når datamaskinen slås på igjen. Denne avmerkingsboksen vises hvis en av følgende kjøremoduser er valgt: **Hver dag** / **Hver uke** / **Hver måned** / **På et bestemt tidspunkt**.
Søk etter programoppdateringer kun når skjermspareren er aktiv eller datamaskinen er låst (Programoppdatering) **Kjør objektanalyse kun når skjermspareren er aktiv eller datamaskinen er låst** (Application Manager)	Kaspersky kjører oppgaven når du er ferdig med å jobbe på datamaskinen. Dermed unngår du at skanneoppgaver bruker opp systemressurser mens du arbeider. Denne avmerkingsboksen vises hvis du har valgt kjøremodusen **Etter hver oppdatering**.

Oppdateringsinnstillinger

Innstillinger	Beskrivelse
Tidsplan for oppdatering av databaser	Når du klikker på denne koblingen, åpnes vinduet **Tidsplan for oppdatering av databaser**, der du kan velge en av kjøremodusene for databaseoppdateringen: **Automatisk**. Kjøremodus for oppdateringsoppgaver, der Kaspersky-programmet søker etter oppdateringspakken i oppdateringskilden ved bestemte intervaller. Skannefrekvensen kan økes ved virusutbrudd og reduseres når det ikke finnes noen. Når Kaspersky-programmet registrerer en ny oppdateringspakke, blir den automatisk lastet ned og installert på datamaskinen. **Manuelt**. Denne kjøremodusen for oppgaver lar deg kjøre oppdateringsoppgaven manuelt. **Hvert minutt** / **Hver time** / **Hver dag** / **Hver uke** / **Hver måned** / **På et bestemt tidspunkt** / **Etter at programmet har startet**. Kjøremodus for oppdateringsoppgaver der Kaspersky-programmet kjører oppdateringsoppgaven i henhold til tidsplanen du har opprettet. Hvis du velger denne kjøremodusen for oppdateringsoppgaver, kan du også kjøre oppdateringsoppgaver for Kaspersky-programmet manuelt.
Velg oppdateringskilder	Når du klikker på denne koblingen, åpnes et vindu med en liste over oppdateringskilder. *En oppdateringskilde* er en offentlig HTTP- eller FTP-server eller en delt mappe (lokal mappe eller nettverksmappe) der programmet kan laste ned oppdateringsdatabaser og moduler. Som standard inneholder listen over oppdateringskilder Kasperskys oppdateringsservere. Du kan legge til andre oppdateringskilder i listen. Hvis flere oppdateringskilder er valgt fra listen, vil Kaspersky-programmet spørre dem etter hverandre til den når den første tilgjengelige oppdateringskilden som den kan laste ned oppdateringspakken fra.
Kjør databaseoppdateringer som	Når du klikker på koblingen, åpnes et vindu der du kan velge å kjøre databaseoppdateringen med rettighetene til en bestemt bruker. Som standard kjøres oppdateringsoppgaven for Kaspersky-programmet i navnet til brukeren som har rettigheter du registrerte i operativsystemet. Kaspersky-programmet kan imidlertid oppdateres fra en oppdateringskilde som brukeren ikke har tilgangsrettigheter til (for eksempel fra en delt mappe som inneholder oppdateringspakken), eller som det ikke er konfigurert godkjenning på proxy-serveren for. Du kan angi en bruker som har de nødvendige rettighetene i Kaspersky-programmet-innstillingene, og deretter kjøre oppdateringsoppgaven for Kaspersky-programmet i navnet til denne brukeren.

Vinduet Sårbarhetsskanning av programmer

Kjør skann

Klikk på denne knappen for å starte Sårbarhetsskanning av programmer.

Stopp

Klikk på denne knappen for å stoppe Sårbarhetsskanning av programmer.

Denne knappen er kun tilgjengelig hvis Sårbarhetsskanning av programmer kjører.

N sårbare programmer

Klikk på denne koblingen for å åpne vinduet **Sårbare programmer**, som inneholder en liste over sårbare programmer som ble oppdaget under skanningen. Denne koblingen vises hvis Sårbarhetsskanning av programmer kjører.

Vinduet Stopp beskyttelsen midlertidig

Stopp midlertidig i

Denne modusen starter beskyttelseskomponentene og aktiverer beskyttelsen igjen etter et angitt tidsintervall.

Du kan spesifisere et tidsintervall i rullegardinlisten under.

Avbryt til programmet startes på nytt

Denne modusen starter beskyttelseskomponentene og aktiverer beskyttelsen igjen når programmet eller operativsystemet startes på nytt (hvis automatisk oppstart av programmet er aktivert).

Stans midlertidig

Denne modusen starter beskyttelseskomponentene og aktiverer beskyttelsen igjen når du ønsker å gjøre det.

Vinduet Passordkontroll

Passord

Passord for å administrere Kaspersky-programmet.

Lagre passordet for gjeldende økt

Hvis dette alternativet er aktivert, vil Kaspersky huske passordet og ikke lenger be om det i gjeldende økt.

Vinduet Programmer tilgang til webkameraet er blokkert for

Dette vinduet viser programmene du har blokkert webkameratilgang for.

Tillat tilgang til webkamera

Klikk på denne knappen for å gi programmet som er valgt i listen, tilgang til webkameraet.

Vinduet Anbefalte innstillinger

Slå på beskyttelse mot annonser for å installere kun ønsket programvare og blokkere ekstra installasjoner

Hvis alternativet velges, vil Kaspersky blokkere visning av annonser når du installerer programvare på datamaskinen. Installasjon av ekstra programvare det reklameres for, blokkeres også.

Fullført

Klikk på denne knappen for å gå til hovedvinduet.

Vinduet Rapporter

Du kan bruke følgende funksjoner for enkel behandling av rapporter:

- Filtrer etter dato.
- Filtrer etter verdi i en vilkårlig celle.
- Søk etter tekst i hendelsesoppføring.
- Sorter listen etter hver rapportkolonne.
- Endre rekkefølgen og sorteringen av kolonner som vises i rapporten.

Følgende viktighetsnivåer for hendelser brukes i rapporter:

Informasjonsmeldinger. Informasjonshendelser som vanligvis ikke inneholder viktig informasjon.

Advarsler. Hendelser som du må ta hensyn til, siden de inneholder informasjon om viktige situasjoner som kan oppstå når du kjører Kaspersky-programmet.

Kristiske hendelser. Viktige hendelser som angir at Kaspersky-programmet har oppdaget problemer som påvirker programmets evne til å kjøre, eller sårbarheter som påvirker beskyttelsesnivået til brukerens datamaskin.

Når du klikker på knappen **Lagre rapport**, kan du lagre rapporten som en TXT- eller CSV-formatfil.

Delen Kontoinnstillinger

Kjør databaseoppdateringer som

Oppdateringsoppgaver for Kaspersky kjøres med rettighetene til brukerkontoen du velger. Denne funksjonen gir deg muligheten til å kjøre en oppdateringsoppgave i Kaspersky både manuelt og i henhold til en tidsplan.

Følgende alternativer er tilgjengelige:

- **Gjeldende bruker**. Rettighetene til gjeldende konto (systemkontoen du er logget på) vil gjelde for oppdateringsoppgaver.
- **Annen bruker**. Oppdateringsoppgaver kjøres under angitte brukerkonto. Hvis du velger dette alternativet, må du angi kontonavn og passord i feltene **Konto** og **Passord**.

Send rapport

Informasjon om operativsystemet

Med denne avmerkingsboksen kan du legge til informasjon om operativsystemets status i rapporten som skal sendes til Teknisk støtte.

Data mottatt til analyse

Ved å merke av for en avmerkingsboks kan du legge til sporingsfiler og minnedumper i rapporten som sendes til Teknisk støtte. Historikk for kjøring av kommandoer for programmet og informasjon om programmets tilstand lagres til disse filene.

Hvis du klikker på koblingen **<antall filer>**, **<datavolum>** ved siden av avmerkingsboksen, åpnes vinduet **Data mottatt til analyse**. Vinduet viser listen over filer og det totale datavolumet som skal overføres til Teknisk støtte.

Lagre rapporten på datamaskinen

Klikk på denne koblingen for å åpne en dialogboks for å lagre filen.

Angi forespørselsnummer

Et nummer som tilordnes forespørselen når du kontakter Teknisk støtte fra My Kasperskys nettsted.

Send rapport

Knapp som laster opp valgte filer til FTP-serveren til Teknisk støtte.

Vinduet Data mottatt til analyse

Liste over datafiler

En filliste som Kaspersky inkluderer i rapporten som sendes til teknisk støtte. Listen inkluderer sporingsfiler og minnedumpfiler. Historikk for kjøring av kommandoer for programmet og informasjon om programmets tilstand lagres til disse filene.

Hvis boksen på fillinjen er aktivert, sendes filen til Teknisk støtte. Datafiler forberedes og pakkes i et arkiv før de lastes opp.

Hvis boksen på fillinjen er deaktivert, sendes filen ikke til Teknisk støtte.

Fil

Denne kolonnen viser navnet på en fil som allerede skal sendes til Teknisk støtte.

Størrelse

Datavolumet som skal sendes til Teknisk støtte dersom den angitte filen er inkludert i rapporten. Programmet inkluderer en fil i rapporten hvis avmerkingsboksen på linjen til denne filen er aktivert.

Kjør skript

Teksten til skriptet som skal kjøres

Skriptteksten som er mottatt fra Teknisk støtte.

Kasperskys eksperter anbefaler at du ikke endrer teksten i skriptet.

Kjør

Klikk på denne knappen for å starte skriptet.

Kjøre AVZ-skript

Dette vinduet viser prosessen for kjøring av AVZ-skript. Skriptkjøring kan ta litt tid.

Resultatet av skriptkjøringen

Feil

Feilmelding. Vises hvis det er funnet feil i AVZ-skriptet. Veiviseren for kjøring av AVZ-skripter stanser.

Fullført

Klikk på denne knappen for å lukke veiviseren for kjøring av AVZ-skripter.

Resultatet av skriptkjøringen

Lukk

Klikk på denne knappen for å lukke veiviseren for kjøring av AVZ-skripter.

Rediger

Klikk på denne knappen for å legge til skriptet og forsøke å kjøre skriptet på nytt.

Vinduet Sårbare programmer

Sårbare programmer

Viser en liste over sårbarheter som er oppdaget i programmer.

På grunn av virkemåten til visse oppdateringstjenester er det mulig at sårbarheter i enkelte programmer oppdages flere ganger.

Følgende knapper er tilgjengelige for hver sårbarhet:

- **Detaljer**

Når du klikker på denne knappen, åpnes nettstedet for teknisk støtte, der du finner en beskrivelse av trusselen. På dette nettstedet kan du laste ned oppdateringer for din versjon av programmet og installere dem.

- **Legg til i unntak**

Når du klikker på denne knappen, legges programmet til i klarert sone.

Velge en ZIP-fil eller mappe

Egendefinerte temaer er ikke tilgjengelige i noen regioner.

Vurder følgende begrensninger når du velger et tema:

- Kaspersky vil ikke kunne bruke det valgte temaet i følgende tilfeller:
  - Filene i arkivet har et navn eller en bane i mappestrukturen som er ulikt fra navnet i standardtemaet.
  - De arkiverte filene som er ansvarlige for tekstene i programvinduet er skadde.
- Teamene er utformet for en bestemt versjon av Kaspersky og gjelder ikke for andre versjoner eller andre programmer. Temaet bytter til standardtemaet når du oppgraderer programmet til en ny versjon eller installerer et annet program over det.

Hvis du støter på problemer når du velger et alternativt tema, og du ikke kan installere standardtemaet med den spesifiserte metoden (for eksempel at du ikke kan fjerne krysset i ruten **Bruk et tema med egendefinert design** i vinduet **Innstillinger for grensesnitt** fordi skriften smelter sammen med bakgrunnen og de nødvendige elementene ikke kan skilles fra hverandre), anbefaler vi å installere Kaspersky på nytt.

Vinduet Legg til / rediger unntak for datamaskintastaturet

Nettadressemaske

Nettadressen til et nettsted du vil legge til i listen. Du kan angi en nettadresse eller en adressemaske.

I delen **Omfang** kan du angi området som unntaksregelen for Sikkert tastaturinput skal gjelde for.

Bruk på hele nettstedet

Sikkert tastaturinput er aktivert for alle sidene på nettstedet som er angitt i feltet **Nettadressemaske**.

Bruk på angitt side

Sikkert Tastaturinput er aktivert kun på websiden som er angitt i feltet **Nettadressemaske**.

I delen **Sikkert tastaturinput** kan du angi om Kaspersky skal beskytte data som tastes inn via datamaskintastaturet, for valgte nettsteder eller websider.

Beskytt

Kaspersky beskytter data som tastes inn via datamaskintastaturet, for valgt webområde eller webside.

Ikke beskytt

Kaspersky beskytter ikke data som tastes inn via datamaskintastaturet, for valgt webområde eller webside.

Vinduet Legg til /rediger unntak for skjermtastatur

Nettadressemaske

Nettadressen til et nettsted du vil legge til i listen. Du kan angi en nettadresse eller en adressemaske.

I delen **Omfang** kan du angi innstillingene for visning av ikonet for Skjermtastatur: Hele nettstedet eller den angitte siden.

Bruk på hele nettstedet

Hurtigstartikonet til Skjermtastatur vises i registreringsfeltene på alle sidene på nettstedet som er angitt i feltet **Nettadressemaske**.

Bruk på angitt side

Hurtigstartikonet til Skjermtastatur vises kun i registreringsfeltene på websiden som er angitt i feltet **Nettadressemaske**.

I delen **Ikon for skjermtastatur** kan du angi om programmet skal vise ikonet til Skjermtastatur på sidene som samsvarer med den angitte nettadressemasken.

Vis ikonet i nettleservinduet

Kaspersky viser hurtigstartikonet for Skjermtastatur i registreringsfeltene.

Ikke vis ikonet i nettleservinduet

Kaspersky viser ikke hurtigstartikonet for Skjermtastatur i registreringsfeltene.

Innstillinger for Rapporter og karantene

I delen **Rapporter** kan du konfigurere innstillingene for opprettelse og lagring av rapporter.

Lagre rapporter i maksimalt

Dette alternativet aktiverer/deaktiverer alternativet som definerer maksimal lagringstid for rapporter. Objekter kan lagres i én dag, én uke, én eller seks måneder eller ett år.

Når den angitte verdien er nådd, sletter programmet alle rapportoppføringe som er eldre enn det angitte antallet dager minus 10 %. Hvis du angir en verdi på 30 dager, og det er en i rapporten som er eldre enn 30 dager, slettes alle hendelser som har vært lagret i mer enn 27 dager fra rapporten.

Hvis det ikke er merket av for alternativet, er ikke oppbevaringstiden for rapporter begrenset.

Begrens størrelsen på rapportfiler til

Avmerkingsboksen aktiverer/deaktiverer alternativet som begrenser maksimalstørrelsen på rapporter. Maksimal filstørrelse er angitt i megabyte.

Hvis alternativet er aktivert, er maksimal rapportstørrelse 1024 MB. Slettingen skjer når halvparten av den angitte størrelsen er nådd. 10 % av rapportfilens faktiske størrelse slettes. Hvis den angitte verdien er 1024 MB, begynner eldre oppføringer i rapportfilen å bli slettet når rapportfilen når 512 MB, og størrelsen på rapportfilen reduseres med 10 % av den faktiske størrelsen ved å slette de eldste oppføringene.

Hvis alternativet er deaktivert, begrenses ikke rapportens filstørrelse.

Tøm

Når du klikker på denne knappen, vil Kaspersky fjerne data fra mappen med rapporter.

Som standard sletter Kaspersky rapportene for skanneoppgaver, oppdateringsrapporter, rapporter om bruk av brannmurregler.

I delen **Karantene** kan du endre innstillinger for Karantene.

Lagre objekter i maksimalt

Dette alternativet aktiverer/deaktiverer alternativet som begrenser lagringstiden for objekter i Karantene. Objekter kan lagres i én dag, én uke, én eller seks måneder eller ett år.

Hvis alternativet er aktivert, lagres objekter i perioden som er valgt fra rullegardinlisten ved siden av avmerkingsboksen.

Hvis avmerkingen for alternativet er fjernet, begrenses ikke lagringstiden for objekter.

Begrens størrelsen på Karantene til

Denne avmerkingsboksen aktiverer/deaktiverer alternativet som definerer maksimalstørrelsen på Karantene. Størrelsen på Karantene er angitt i megabyte.

Hvis boksen er aktivert, er standard maksimal størrelse 100 MB. Når maksimal størrelse overskrides, fjernes de eldste objektene og nye legges til.

Hvis boksen ikke er avkrysset, er lagringsstørrelsen ubegrenset.

Innstillinger for Selvforsvar

Aktiver Selvforsvar

Dette alternativet aktiverer/deaktiverer beskyttelsesmekanismene til Kaspersky-programmet mot endringer eller sletting av egne filer fra harddisken, minneprosesser og oppføringer i systemregisteret.

Hvis det er merket av for denne boksen, er tjenesten for ekstern kontroll av systemet også deaktivert. Hvis tjenesten for ekstern kontroll av systemet er deaktivert, vil Kaspersky-programmet blokkere alle eksterne forsøk på å styre programmer. Hvis et forsøk på å styre programmet eksternt oppdages, vises en varsling over ikonet for Kaspersky-programmet i systemstatusfeltet i Microsoft® Windows® (hvis varslinger ikke er deaktivert).

Tillat administrering av innstillingene for <PRODUCT> via fjernstyringsprogrammer

Hvis dette alternativet er valgt, vil klarerte fjernstyringsprogrammer (f.eks. TeamViewer, LogMeIn Pro og Remotely Anywhere) kunne endre innstillingene for Kaspersky.

Ikke klarerte fjernstyringsprogrammer vil ikke kunne endre innstillingene for Kaspersky, selv om dette alternativet er valgt.

Proxy-serverinnstillinger

Ikke bruk proxy-server

Denne knappen aktiverer/deaktiverer bruk av en proxy-server for Internett-tilkoblinger. Du må være tilkoblet Internett for å kunne bruke enkelte beskyttelseskomponenter i Kaspersky og for å oppdatere databaser og programmoduler.

Registrer innstillingene til proxy-serveren automatisk

Kaspersky kontrollerer automatisk innstillingene til proxyserveren ved å bruke WPAD (Web Proxy Auto-Discovery Protocol).

Hvis denne protokollen ikke kan fastsette adressen, bruker Kaspersky proxy-serverinnstillingene angitt i den Chromium-baserte nettleseren Microsoft Edge. Kaspersky tar ikke hensyn til proxy-serverinnstillinger som er angitt for andre nettlesere som er installert på brukerens datamaskin.

Bruk angitte proxy-serverinnstillinger

Kaspersky bruker en annen proxy-server enn den som er angitt i nettleserens tilkoblingsinnstillinger.

Adresse

Inneholder IP-adressen eller det symbolske navnet (URL-adressen) til en proxy-server.

Feltet er redigerbart dersom innstillingen **Bruk angitte proxy-serverinnstillinger** er valgt (for eksempel IP 192.168.0.1).

Port

Proxyserverens port.

Feltet er tilgjengelig hvis innstillingen **Bruk angitte proxy-serverinnstillinger** er valgt.

Bruk proxy-servergodkjenning

Godkjenning er verifisering av brukerens påloggingsdata.

Denne boksen aktiverer/deaktiverer bruk av godkjenning på proxyserveren.

Hvis alternativet er aktivert, forsøker Kaspersky først å utføre NTLM-godkjenning, og deretter enkel (BASIC) godkjenning.

Hvis alternativet er deaktivert, eller det ikke er angitt innstillinger for proxy-server, forsøker Kaspersky å utføre NTLM-godkjenning ved hjelp av kontoen oppgaven er kjørt under (for eksempel en oppdateringsoppgave).

Hvis proxy-serveren krever autentisering, og brukernavn og passord ikke er angitt, eller hvis angitte data ikke er godkjent av proxy-serveren, vises et vindu som ber om brukernavn og passord. Ved vellykket godkjenning vil Kaspersky bruke angitt brukernavn og passord i fremtiden. Hvis ikke vil Kaspersky be deg om å angi innstillinger for autentisering igjen.

Brukernavn

Brukernavnet som brukes for godkjenning på proxyserveren.

Passord

Passordet for det angitte brukernavnet.

Omgå proxy-server for lokale adresser

Hvis alternativet er aktivert, bruker ikke Kaspersky proxy-serveren ved oppdatering av databaser og programvaremoduler fra en lokal mappe eller nettverksmappe.

Hvis alternativet ikke er aktivert, bruker Kaspersky proxy-serveren ved oppdatering av databaser og programvaremoduler fra en lokal mappe eller nettverksmappe.

Delen Beskyttelse

Listen Beskyttelseskomponenter

Denne listen inkluderer beskyttelseskomponenter utformet for å gi beskyttelse mot ulike typer digitale trusler.

Hver enkelt trusseltype behandles av en bestemt komponent. Komponentene kan aktiveres og deaktiveres uavhengig av hverandre, og innstillingene kan konfigureres.

Webkamera og mikrofonkontroll

Aktiver/deaktiver Webkamera og mikrofonkontroll

Denne bryteren aktiverer/deaktiverer Webkamera og mikrofonkontroll.

Under **Webkamera-innstillinger** kan du redigere følgende innstillinger:

Blokker tilgang til webkameraet for alle programmer

Hvis dette alternativet er valgt, er tilgang til webkamera blokkert for alle programmer som er installert på datamaskinen.

Varsle hvis et program bruker webkameraet

Hvis dette alternativet er valgt, vil Kaspersky vise en varsling når et program som har tilgang, bruker webkameraet. I varslingsvinduet kan du redigere innstillingene for programmets tilgang til webkameraet, eller velge å ikke motta flere varslinger.

Under **Mikrofoninnstillinger** kan du redigere følgende innstillinger:

Blokker tilgang til mikrofonen for alle programmer

Hvis dette alternativet er valgt, er tilgang til mikrofonen blokkert for alle programmer som er installert på datamaskinen.

Varsle hvis et program bruker mikrofonen

Hvis dette alternativet er valgt, vil Kaspersky vise en varsling når et program som har tilgang, bruker mikrofonen. I varslingsvinduet kan du redigere innstillingene for programmets tilgang til mikrofonen, eller velge å ikke motta flere varslinger.

Lær mer om Webkamera og mikrofonkontroll

Mistenkelig omdirigering oppdaget

Slett oppføringer

Kaspersky sletter alle mistenkelige oppføringer fra vertsfilen.

Hopp over

Kaspersky sletter ikke mistenkelige oppføringer i listen fra vertsfilen, dersom de er angitt på listen.

Liste over mistenkelige oppføringer

Denne listen inneholder adressene til skadelige eller ukjente webservere som du omdirigeres til når programmet forsøker å koble til Kasperskys servere.

Vi anbefaler at du sletter alle mistenkelige oppføringer fra vertsfilen.

Vindu for inntasting av passord

Gjeldende passord

Det gjeldende passordet brukes for tilgang til administrasjon av Kaspersky.

Lagre passordet for gjeldende økt

Hvis dette alternativet er aktivert, vil Kaspersky huske passordet og ikke lenger be om det i gjeldende økt.

Vinduet Passordbeskyttelse

Koblingen **Endre eller fjerne passord** er tilgjengelig hvis det er angitt et passord for å beskytte tilgang til funksjonene i Kaspersky.

Endre eller fjerne passord

Når du klikker på denne koblingen, vil du se felter for å angi et nytt passord og bekrefte dette passordet.

Nytt passord

Passord for administrering av Kaspersky.

Bekreft passord

Tast inn passordet du har angitt i feltet **Nytt passord** på nytt.

I delen **Passordomfang** kan du angi hvilke deler av programbehandlingen som skal passordbeskyttes.

Konfigurer programinnstillinger

Alternativet aktiverer/deaktiverer anmodning om passord når brukeren forsøker å lagre endringer i programinnstillingene.

Styre sikkerhetskopiering og gjenoppretting

Denne avmerkingsboksen aktiverer/deaktiverer alternativet som ber brukeren om å angi et passord for å åpne vinduet **Sikkerhetskopiering og gjenoppretting**.

Avslutt programmet

Alternativet aktiverer/deaktiverer anmodning om passord når brukeren forsøker å avslutte programmet.

Fjerne programmet

Alternativet aktiverer / deaktiverer anmodning om passord når brukeren forsøker å fjerne programmet.

Skanneinnstillinger

Tabellen beskriver innstillingene som kontrollerer følgende skannetyper: Fullstendig skann, Hurtigskann, Selektivt skann og Umiddelbar filskanning.

Innstillinger	Beskrivelse
Sikkerhetsnivå	Kaspersky bruker forskjellige sett med innstillinger for skanning. Innstillingene som er lagret i programmet, kalles *sikkerhetsnivåer*. • **Ekstremt**. Kaspersky-programmet skanner alle typer filer. Ved skanning av sammensatte filer vil programmet også skanne filer i e-postformat. • **Optimalt**. Kaspersky-programmet skanner bare angitte filformater på alle harddisker, nettverksstasjoner, flyttbare lagringsmedier på datamaskinen og innebygde OLE-objekter. Programmet skanner ikke arkiver og installasjonspakker. • **Lavt**. Kaspersky-programmet skanner bare nye og endrede filer med visse filtyper på alle datamaskinens harddisker, flyttbare stasjoner og nettverksstasjoner. Programmet skanner ikke sammensatte filer.

Handling ved oppdagelse av trussel	• **Spør brukeren**. Hvis Kaspersky-programmet oppdager et infisert eller potensielt infisert objekt under en skanning, varsles du umiddelbart om denne hendelsen. Du blir også bedt om velge hvilken handling som skal utføres på de oppdagede objektene.
	Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er deaktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**.
	• **Velg handling automatisk**. Når det oppdages infiserte eller potensielt infiserte objekter, utfører Kaspersky handlingene som er anbefalt av Kasperskys eksperter:
	  • Kaspersky prøver først å desinfisere et infisert objekt. Hvis desinfisering ikke er mulig, sletter det filen.
	  • Kaspersky sletter et potensielt infisert objekt hvis avmerkingsboksen **Slett skadelige verktøy, annonseprogrammer, programmer som automatisk foretar anrop og mistenkelige pakker** er valgt. Hvis alternativet er deaktivert, sletter ikke programmet et potensielt infisert objekt. I stedet vises et varsel om påvisning av dette objektet i varslingssenteret (klikk på **Detaljer** i hovedprogramvinduet for å åpne det).
	Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er valgt under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**.
	• **Desinfiser, slett hvis desinfisering ikke er mulig**. Hvis dette alternativet er valgt, prøver programmet automatisk å desinfisere alle infiserte filer som er funnet. Hvis desinfisering ikke er mulig, sletter programmet objektene.
	• **Desinfiser, blokker hvis desinfisering ikke er mulig**. Hvis du velger denne handlingen, prøver Kaspersky automatisk å desinfisere alle infiserte filer som den finner. Hvis desinfiseringen mislykkes, legger programmet til informasjon om de infiserte filene den finner på listen over detekterte objekter.
	• **Varsle**. Hvis dette alternativet er valgt, legger Kaspersky-programmet til informasjon om de infiserte filene den finner på listen over detekterte objekter.

	Når du prøver å desinfisere eller slette en infisert fil, oppretter programmet først en sikkerhetskopi i tilfelle du trenger å gjenopprette filen, eller det blir mulig å desinfisere den, senere.
Rediger skanneomfang (ikke tilgjengelig i innstillingene for Skanning av hurtigmeny)	Når du klikker på koblingen, åpnes et vindu med en liste over objekter som Kaspersky-programmet kan skanne. Ulike objekter inkluderes som standard i listen avhengig av skannetype (Fullstendig skann, Hurtigskann eller Selektivt skann). Du kan legge til objekter i listen eller slette objektene du legger til. Hvis du vil fjerne et objekt fra skanningen, trenger du ikke å slette objektet fra listen. Du trenger bare å fjerne avmerkingen i boksen ved siden av objektnavnet.
Skannetidsplan (ikke tilgjengelig i innstillingene for Skanning av hurtigmeny)	**Manuelt**. Kjøremodus der du kan skanne manuelt når det passer for deg. **Etter tidsplan**. En skannekjøremodus der programmet kjører skanneoppgaven etter tidsplanen du har opprettet. Hvis du velger denne skannekjøremodusen, kan du også kjøre skanneoppgaven manuelt.
Kjør skanning som	Når du klikker på koblingen, åpnes et vindu der du kan velge å kjøre skanningen ved å bruke rettighetene til en bestemt bruker. Som standard kjøres skanneoppgaven i navnet til brukeren med rettighetene som du har registrert i operativsystemet. Beskyttelsesomfanget kan omfatte nettverksstasjoner eller andre objekter som krever spesielle tilgangsrettigheter. Du kan angi en bruker som har de nødvendige rettighetene, i innstillingene for programmet og kjøre skanneoppgaven på vegne av denne brukeren.
Filtyper	Kaspersky-programmet håndterer filer uten forlengelser som kjørbare. Programmet skanner alltid slike filer, uavhengig av filtypene du har valgt å skanne. **Alle filer**. Hvis denne innstillingen er aktivert, skanner Kaspersky alle filer uten unntak (alle formater og filtyper). **Filer skannet etter format**. Hvis du velger denne innstillingen, skanner programmet kun potensielt infiserte filer. Før du søker etter skadelig kode i en fil, analyseres filens interne filhode for å fastsette filformatet (TXT, DOC, EXE osv.). Skanningen ser også etter filer med bestemte filtyper. **Filer skannet etter filtype**. Hvis du velger denne innstillingen, skanner programmet kun potensielt infiserte filer. Filformatet gjenkjennes ved hjelp av filtypen.
Skann kun nye og endrede filer	Skanner bare nye filer og filene som er endret siden sist de ble skannet sist. På denne måten kan du spare tid på skanningen. Denne skannemodusen gjelder både for enkle og sammensatte filer.
Hopp over objekter skannet lengre enn N sekunder	Begrenser varigheten for skanning av et enkelt objekt. Når den angitte tiden har utløpt, stopper programmet filskanningen. På denne måten kan du spare tid på skanningen.
Skann arkiver	Skann ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE og andre arkiver. Programmet skanner arkiver ikke bare etter utvidelsene, men også etter formatene deres.
Skann distribusjonspakker	Avmerkingsboksen aktiverer/deaktiverer skanning av distribusjonspakker fra tredjeparter.
Skann filer med Microsoft Office-format	Skanner Microsoft Office-filer (DOC, DOCX, XLS, PPT og andre Microsoft-filtyper). Microsoft Office-filer inkluderer også OLE-objekter.

Skann e-postformater	Boksen aktiverer / deaktiverer alternativet i Kaspersky for skanning av filer i e-postformater og e-postdatabaser. Programmet kjører kun fullstendige skanninger av e-postfilformatene Microsoft Outlook, Windows Mail / Microsoft Outlook Express og EML, og bare hvis datamaskinen kjører e-postklienten Microsoft Outlook x86. Hvis det er merket av for dette alternativet, dekonstruerer Kaspersky e-postformatfilen og analyserer hvert komponent (meldingstekst, vedlegg) for virus. Hvis boksen ikke er avkrysset, skanner Kaspersky e-postformatet som et enkelt objekt.
Gjennomsøk passordbeskyttede arkiver	Hvis avmerkingsboksen er aktivert, skanner programmet passordbeskyttede arkiver. En dialogboks som ber deg om å oppgi et passord, vises på skjermen før du kan skanne filene i arkivet. Hvis avmerkingsboksen ikke er aktivert, skanner ikke programmet passordbeskyttede arkiver.
Ikke pakk ut store sammensatte filer **Maksimal filstørrelse**	Hvis avmerkingsboksen er valgt, skanner ikke programmet sammensatte filer som er større enn den angitte verdien. Hvis alternativet er deaktivert, skanner programmet sammensatte filer av enhver størrelse. Programmet skanner store filer som er hentet fra arkiver, uavhengig av om avmerkingsboksen er aktivert eller ikke.
Heuristisk analyse	En teknikk for å oppdage trusler som ikke kan identifiseres ved å bruke den gjeldende versjonen av programdatabasene til Kaspersky. Den lar deg finne filer som kan inneholde ukjent skadelig programvare eller en ny modifisering av kjent skadelig programvare. Når du skanner filer etter skadelig kode, utfører den heuristiske analysen instruksjoner i de kjørbare filene. Antall instruksjoner som utføres av den heuristiske analysen, avhenger av nivået som er angitt for den heuristiske analysen. Det heuristiske analysenivået angir balansen mellom grundighetsnivået på søket etter nye trusler, belastningen på operativsystemets ressurser og tiden som kreves for den heuristiske analysen.
iSwift-teknologi	Denne teknologien er en videreutvikling av iChecker-teknologi for datamaskiner som benytter NTFS-filsystemet. Det finnes begrensninger med iSwift-teknologien: Den er knyttet til en bestemt fils plassering i filsystemet og kan kun brukes for objekter i NTFS-filsystemet. Når du oppgraderer Kaspersky-programmet til en ny versjon, er iSwift-teknologien aktivert for alle typer skanning, selv om den tidligere var deaktivert.
iChecker-teknologi	Denne teknologien gjør det mulig å øke skannehastigheten ved å utelate bestemte filer fra skanning. En fil utelates fra skanning med en spesiell algoritme som tar hensyn til utgivelsesdatoen for Kaspersky-programmets databaser, datoen filen sist ble skannet og eventuelle endringer gjort for skanneinnstillingene. Det finnes begrensninger med iChecker-teknologien: Den fungerer ikke med store filer og gjelder kun for filer med en struktur som programmet gjenkjenner (for eksempel EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP og RAR).

Skanneinnstillinger for flyttbare stasjoner

Innstillinger	Beskrivelse
Handling når eksterne enheter kobles til	• **Hurtigskann**. Hvis du velger dette alternativet og kobler til en enhet, skanner Kaspersky bare filer med bestemte formater som er mest sårbare for infeksjon og er plassert i rotmappen. Hurtigskann inkluderer ikke dekomprimering og skanning av arkiver. • **Detaljert skanning**. Hvis det er merket av for dette alternativet, skanner Kaspersky alle filene i hver mappe på den eksterne enheten etter at du har koblet til en ekstern enhet. Det dekomprimerer og skanner i tillegg arkiver, bortsett fra de som er beskyttet med passord.
Maksimal størrelse for eksterne enheter	Hvis avmerkingsboksen er valgt, skanner Kaspersky alle eksterne enheter som ikke overskrider den angitte maksimalstørrelsen. Hvis avmerkingsboksen er deaktivert, skanner Kaspersky eksterne enheter i alle størrelser.
Vis skanningens fremgang	Hvis det er merket av for dette alternativet, viser Kaspersky fremdriften til skanninger av eksterne enheter i et eget vindu og i vinduet for den aktive skanningen.
Blokker stopping av skanneoppgaven	Hvis det er merket av for dette alternativet, er ikke **Stopp**-knappen tilgjengelig for skanning av eksterne enheter i det aktive skannevinduet.

Innstillinger for bakgrunnsskanning

Hvis bakgrunnsskanning er aktivert, vil Kaspersky kjøre bakgrunnsskanning. En bakgrunnsskanning er en automatisk skannemodus som ikke viser varsler. Denne skanningen bruker færre datamaskinressurser enn andre typer skanninger (for eksempel Fullstendig skanning). I denne modusen skanner Kaspersky systemminnet, systemvolumer, bootsektorer og oppstartsobjekter, og søker etter rootkits.

Hvis datamaskinen er batteridrevet, kjører ikke Kaspersky bakgrunnsskanning når datamaskinen er inaktiv.

Innstillinger for Sårbarhetsskanning av programmer

Innstillinger	Beskrivelse
Rediger skanneomfang	Når du klikker på koblingen, åpnes vinduet **Omfang for sårbarhetsskanning av programmer** med en liste over objekter som skannes for sårbarheter i programmer. Du kan legge til objekter i listen eller slette objektene du legger til. Hvis du vil fjerne et objekt fra skanningen, trenger du ikke å slette objektet fra listen. Du trenger bare å fjerne avmerkingen i boksen ved siden av objektnavnet.
Tidsplan for søk	**Manuelt**. Kjøremodus der du kan starte Sårbarhetsskanning av programmer manuelt når det passer deg. **Etter tidsplan**. En skannekjøremodus der programmet kjører skanneoppgaven etter tidsplanen du har opprettet. Hvis du velger denne skannekjøremodusen, kan du også kjøre skanneoppgaven manuelt.

Kontoinnstillinger

Kjør skanning som

Velg en konto med rettighetene som skal brukes av Kaspersky ved kjøring av skanneoppgaver. Funksjonen er tilgjengelig både for manuell skanning og planlagt skanning.

Følgende alternativer er tilgjengelige:

- **Gjeldende bruker**. Skanneoppgaver kjøres med rettighetene til gjeldende konto.
- **Annen bruker**. Angitt brukerkonto vil brukes til å kjøre skanneoppgaver. Hvis du velger dette alternativet, må du skrive inn kontonavn og passord i feltene **Konto** og **Passord**.

Innstillinger for Anti-Banner

Aktiver/deaktiver Anti-Banner

Denne bryteren aktiverer/deaktiverer Anti-Banner.

Hvis knappen er grønn, viser Anti-Banner bannere på nettstedene du besøker, samt i grensesnittene til bestemte programmer. Som standard vil Anti-Banner blokkere nettsteder fra listen med kjente bannere. Denne listen er inkludert i databasene til Kaspersky.

Liste over filtre

Ved å klikke på denne lenken åpnes vinduet **Liste over filtre**, der du kan bruke spesielle filtre til å spesifisere nærmere nøyaktig hvilke bannere som må blokkeres.

Nettsteder med tillatte bannere

Klikk på denne koblingen for å åpne et vindu med en liste over nettsteder du har tillatt at det vises bannere på.

Blokkerte bannere

Ved å klikke på denne lenken åpnes vinduet **Blokkerte bannere**. Du kan bruke dette vinduet til å opprette en liste med bannere som skal blokkeres.

Tillatte bannere

Ved å klikke på denne lenken åpnes vinduet **Tillatte bannere**. Du kan bruke dette vinduet til å opprette en liste med bannere som skal tillates.

Tillat bannere på Kasperskys nettsteder

Hvis dette alternativet er valgt, vil Anti-Banner ikke blokkere bannere på nettstedene til Kaspersky og dets partnere som inneholder Kaspersky-annonser. En liste over disse nettstedene er tilgjengelige via koblingen **Kasperskys nettsteder**.

Kasperskys nettsteder

Klikk på denne koblingen for å åpne et vindu med en liste over Kasperskys nettsteder.

Koblingen er tilgjengelig hvis alternativet **Tillat bannere på Kasperskys nettsteder** er aktivert.

Vinduet Legg til / rediger banner

Nettadressemaske (URL)

IP-adresse, nettadresse (URL) eller nettadressemaske.

Når du angir en nettadressemaske, kan du bruke jokertegnene `*` og `?`, der `*`representerer en hvilket som helst tegnkombinasjon og `?` står for et hvilket som helst tegn.

Status

I **Status**-delen kan du angi om Anti-Banner skal bruke denne adressen ved skanning av bannere.

Følgende alternativer er tilgjengelige:

- **Aktiv**. Anti-Banner bruker denne adressen ved skanning av bannere.
- **Inaktiv**. Anti-Banner bruker ikke denne adressen ved skanning av bannere.

Vinduet Legg til / rediger nettsted

Nettsted

Nettstedets nettadresse (URL).

Status

Delen **Status** lar deg spesifisere om Anti-Banner må tillate visning av bannere på det spesifiserte nettstedet.

Følgende alternativer er tilgjengelige:

- **Aktiv**. Anti-Banner tillater visning av bannere på det spesifiserte nettstedet.
- **Inaktiv**. Anti-Banner tillater ikke visning av bannere på det spesifiserte nettstedet.

Vinduet Blokkerte bannere

Knappen

Klikk på denne knappen for å åpne en meny med følgende menyelementer:

- **Importer og legg til i eksisterende**. Dette elementet åpner et vindu der du kan importere en liste over blokkerte adresser fra en CSV-fil. Gjeldende adresser slettes ikke.
- **Importer og erstatt eksisterende**. Dette elementet åpner et vindu der du kan importere en liste over blokkerte adresser fra en CSV-fil. De gjeldende adressene slettes.
- **Eksporter**. Dette elementet åpner et vindu der du kan eksportere en liste over blokkerte adresser til en CSV-fil.

Liste over blokkerte bannere

Butikkadresser eller adressemasker for blokkerte bannere. Anti-Banner blokkerer en banner hvis adressen er i listen over blokkerte bannere.

Du kan legge til en adresse eller adressemaske i listen.

Hvis verdien *Aktiv* er angitt på adresselinjen i **Status**-kolonnen, bruker Anti-Banner denne adressen ved skanning av bannere.

Hvis verdien *Inaktiv* er angitt på adresselinjen i **Status**-kolonnen, bruker ikke Anti-Banner denne adressen ved skanning av bannere.

Nettadressemaske (URL)

Denne kolonnen viser adressen eller adressemasken til det blokkerte banneret.

Status

Denne kolonnen viser om Anti-Banner bruker denne adressen ved skanning av bannere.

Hvis verdien *Aktiv* er angitt på adresselinjen, bruker Anti-Banner denne adressen ved skanning av bannere.

Hvis verdien *Inaktiv* er angitt på adresselinjen, bruker ikke Anti-Banner denne adressen ved skanning av bannere.

Rediger

Klikk på denne knappen for å åpne et vindu der du kan endre adressen eller adressemasken til et banner i listen over blokkerte bannere.

Slett

Som får Anti-Banner til å fjerne den valgte adressen/adressemasken fra listen.

Legg til

Klikk på denne knappen for å åpne et vindu der du kan legge til adressen eller adressemasken til et banner i listen over blokkerte bannere.

Vinduet Tillatte bannere

Knappen

Klikk på denne knappen for å åpne en meny med følgende menyelementer:

- **Importer og legg til i eksisterende**. Velg dette elementet hvis du vil importere en liste over tillatte adresser fra en CSV-fil. Gjeldende adresser slettes ikke.
- **Importer og erstatt eksisterende**. Velg dette elementet hvis du vil importere en liste over tillatte adresser fra en CSV-fil. De gjeldende adressene slettes.
- **Eksporter**. Velg dette elementet hvis du vil eksportere en liste over adresser til en CSV-fil. Du kan eksportere den komplette adresselisten eller individuelle adresser valgt fra listen.

Liste over tillatte bannere

Butikkadresser eller adressemasker for tillatte bannere. Anti-Banner vil ikke blokkere et banner hvis adressen er i listen over tillatte adresser.

Du kan legge til en adresse eller adressemaske i listen.

Hvis verdien *Aktiv* er angitt på adresselinjen i **Status**-kolonnen, bruker Anti-Banner denne adressen ved skanning av bannere.

Hvis verdien *Inaktiv* er angitt på adresselinjen i **Status**-kolonnen, bruker ikke Anti-Banner denne adressen ved skanning av bannere.

Nettadressemaske (URL)

Denne kolonnen viser adressen eller adressemasken til det tillatte banneret.

Status

Denne kolonnen viser om Anti-Banner bruker denne adressen ved skanning av bannere.

Hvis verdien *Aktiv* er angitt på adresselinjen, bruker Anti-Banner denne adressen ved skanning av bannere.

Hvis verdien *Inaktiv* er angitt på adresselinjen, bruker ikke Anti-Banner denne adressen ved skanning av bannere.

Rediger

Klikk på denne knappen for å åpne et vindu der du kan endre adressen eller adressemasken til et banner i listen over tillatte bannere.

Slett

Når du klikker på denne knappen, fjerner Anti-Banner den valgte banneradressen/adressemasken fra listen over tillatte bannere.

Legg til

Klikk på denne knappen for å åpne et vindu der du kan legge til adressen eller adressemasken til et banner i listen over tillatte bannere.

Vinduet Nettsteder med tillatte bannere

Knappen

Klikk på denne knappen for å åpne en meny med følgende menyelementer:

- **Importer og legg til i eksisterende**. Velg dette elementet hvis du vil importere en liste over tillatte adresser fra en CSV-fil. Gjeldende adresser slettes ikke.
- **Importer og erstatt eksisterende**. Velg dette elementet hvis du vil importere en liste over tillatte adresser fra en CSV-fil. De gjeldende adressene slettes.
- **Eksporter**. Velg dette elementet hvis du vil eksportere en liste over adresser til en CSV-fil. Du kan eksportere den komplette adresselisten eller individuelle adresser valgt fra listen.

Liste over nettsteder med tillatte bannere

Inneholder adressene til nettsteder du har tillatt at det vises bannere på. Anti-Banner blokkerer ikke bannere på et nettsted hvis nettstedets adresse er i listen.

Hvis verdien *Aktiv* er angitt på adresselinjen i **Status**-kolonnen, tillater Anti-Banner visning av bannere på dette nettstedet.

Hvis verdien *Inaktiv* er angitt på adresselinjen i **Status**-kolonnen, blokkerer Anti-Banner visning av bannere på dette nettstedet.

Rediger

Klikk på denne knappen for å åpne et vindu der du kan endre adressen som er valgt i listen.

Slett

Klikk på denne knappen hvis du vil at Anti-Banner skal fjerne den valgte nettadressen fra listen.

Legg til

Klikk på denne knappen for å åpne et vindu der du kan legge til en nettadresse i listen.

Vinduet Kasperskys nettsteder

Dette vinduet viser en liste med nettstedene til Kaspersky og dets partnere som inneholder Kaspersky-annonser.

Denne listen er kompilert og oppdatert av Kasperskys eksperter. Listen oppdateres automatisk når databaser og programmoduler oppdateres.

Innstillinger for Anti-Spam

Aktiver/deaktiver Anti-Spam

Denne bryteren aktiverer/deaktiverer Anti-Spam.

Hvis knappen er aktivert, vil Anti-Spam gjenkjenne uønsket e-post (spam), og behandle den i henhold til reglene i e-postklienten.

Sikkerhetsnivå

I **Sikkerhetsnivå** kan du velge en av de forhåndsdefinerte innstillingene (sikkerhetsnivåene) for Anti-Spam. Hvilket sikkerhetsnivå du bør velge, avhenger av driftsforholdene og den aktuelle situasjonen.

Følgende sikkerhetsnivåer er tilgjengelige:

- **Ekstremt**. På dette sikkerhetsnivået bruker Anti-Spam maksimal overvåking ved filtrering av spam.

Vi anbefaler at du velger det høyeste sikkerhetsnivået når du arbeider i et farlig miljø (for eksempel når du bruker en gratis e-posttjeneste).

Når du angir et høyt sikkerhetsnivå, kan det føre til at flere meldinger som ikke er spam, kategoriseres som spam.

- **Optimalt**. Dette sikkerhetsnivået gir god balanse mellom ytelse og sikkerhet. Nivået er egnet i de fleste situasjoner.
- **Lavt**. På dette sikkerhetsnivået bruker Anti-Spam et minimalt filtreringsnivå for spam.

Vi anbefaler at du stiller inn et lavt sikkerhetsnivå hvis du arbeider i et trygt miljø (for eksempel ved bruk av kryptert bedrifts-e-post).

Når du angir et lavt sikkerhetsnivå, vil færre meldinger som ikke er spam, kategoriseres som spam eller mulig spam.

Gjenopprett optimalt sikkerhetsnivå

Klikk på denne koblingen hvis du vil at Kaspersky skal bruke **Optimalt** som sikkerhetsnivå. Koblingen vises hvis du har endret innstillingene i vinduet **Avanserte innstillinger for Anti-Spam** i delen **Klassifiser en melding som ikke spam**.

Avanserte innstillinger

Denne koblingen åpner vinduet Avanserte innstillinger for Anti-Spam.

Avanserte innstillinger for Anti-Spam

I delen **Klassifiser en melding som spam** kan du definere betingelser for e-postfiltrering, som Anti-Spam skal bruke til å gjenkjenne spam.

Hvis den inneholder phishing-elementer

Denne boksen aktiverer/deaktiverer skanning av e-postmeldinger for phishing-elementer i teksten eller URLer inkludert i listen over phishing-adresser.

Hvis boksen er aktivert, vil Anti-Spam gjenkjenne meldinger som spam hvis de inneholder URL-adresser fra listen over phishing-adresser.

Hvis boksen er deaktivert, sjekker ikke Anti-Spam meldingens URL-adresser mot listen over phishing-adresser.

Hvis den inneholder URL-adresser fra databasen over skadelige URL-adresser

Denne avmerkingsboksen aktiverer/deaktiverer kontroll av koblinger i meldinger for å sjekke om de er på listen over skadelige nettadresser.

Hvis den er fra en blokkert avsender

Denne avmerkingsboksen aktiverer/deaktiverer e-postfiltrering ved hjelp av listen over blokkerte avsendere. Anti-Spam vil klassifisere meldinger fra disse avsenderne som spam.

Velg

Når du klikker på denne koblingen, åpnes vinduet **Blokkerte avsendere**. Her kan du opprette en liste over blokkerte avsendere.

Du kan angi både adresser og adressemasker for blokkerte avsendere når du oppretter listen.

Koblingen er tilgjengelig hvis alternativet **Hvis den er fra en blokkert avsender** er aktivert.

Hvis den inneholder blokkerte uttrykk

Denne boksen aktiverer/deaktiverer filtrering av meldinger basert på en liste med blokkerte uttrykk. Hvis disse uttrykkene finnes i en melding, angir dette at meldingen er spam.

Velg

Når du klikker på denne knappen, åpnes vinduet **Blokkerte uttrykk**. Her kan du opprette en liste over blokkerte uttrykk.

Du kan angi både blokkerte uttrykk og uttrykksmasker når du oppretter listen.

Koblingen er tilgjengelig hvis det er merket av for alternativet **Hvis den inneholder blokkerte uttrykk**.

Hvis den inneholder obskøne ord

Ved å klikke på denne lenken åpnes vinduet **Grovt språk**. I dette vinduet kan du opprette en liste over uanstendige ord. Hvis slike ord finnes i en melding, angir dette at meldingen er spam.

Denne koblingen er tilgjengelig hvis det er merket av for alternativet **Hvis den inneholder obskøne ord**.

I delen **Klassifiser en melding som ikke spam** kan du definere kjennetegnene som Anti-Spam skal bruke til å gjenkjenne e-post som ikke er spam.

Hvis den er fra en tillatt avsender

Denne boksen aktiverer/deaktiverer kontroll av en avsenderadresse for å se om den er på listen over tillatte avsendere.

Hvis boksen er aktivert, anser Anti-Spam meldinger fra tillatte avsendere som nyttige.

Hvis avmerkingen for alternativet er fjernet, klassifiserer ikke Anti-Spam meldinger fra tillatte avsendere som ikke-spam. Meldinger som er sendt fra avsendere på listen over tillatte avsendere, filtreres ikke.

Velg

Når du klikker på denne koblingen, åpnes vinduet **Tillatte avsendere**. Her kan du opprette en liste over tillatte avsendere.

Du kan angi både adresser til tillatte avsendere og adressemasker når du oppretter listen.

Koblingen er tilgjengelig hvis det er merket av for alternativet **Hvis den er fra en tillatt avsender**.

Hvis den inneholder tillatte uttrykk

Boksen aktiverer/deaktiverer kontroll av en melding opp mot listen over tillatte uttrykk.

Hvis alternativet er aktivert, vil Anti-Spam klassifisere meldinger som nyttige ved å bruke listen over uttrykk.

Hvis alternativet er deaktivert, vil Anti-Spam ikke bruke listen over tillatte uttrykk til å filtrere meldinger, og klassifiserer ikke e-post som nyttig dersom meldingene inneholder uttrykk fra listen.

Velg

Når du klikker på denne koblingen, åpnes vinduet **Tillatte uttrykk**. Her kan du opprette en liste over tillatte uttrykk.

Du kan bruke både individuelle uttrykk og masker for tillatte uttrykk når du oppretter listen.

Koblingen er tilgjengelig hvis det er merket av for alternativet **Hvis den inneholder tillatte uttrykk**.

I delen **Handlinger med meldinger** kan du angi hvilke tagger som skal legges til i emnefeltet til meldinger som Anti-Spam har tilordnet statusen *Spam* eller *Sannsynlig spam*.

Legg til etikett [!! SPAM] i emnet til meldinger klassifisert som spam

Automatisk tilføyelse av en tekstetikett i Emne-feltet i meldinger som Anti-Spam identifiserer som *Spam*.

Etikettens tekst vises i feltet ved siden av avmerkingsboksen. **[!! SPAM]**-etiketten legges til som standard.

Legg til etikett [?? Sannsynlig SPAM] i emnet til meldinger klassifisert som sannsynlig spam

Automatisk tilføyelse av en tekstetikett i Emne-feltet i meldinger som Anti-Spam identifiserer som *Sannsynlig spam*.

Etikettens tekst vises i feltet ved siden av avmerkingsboksen. **[?? Probable SPAM]**-etiketten legges til som standard.

Vinduet Legg til / rediger blokkerte uttrykk

Uttrykksmaske

Uttrykk eller uttrykksmasker som anses å være tegn på spam hvis de oppdages i en melding.

Vektkoeffisient for uttrykk

En numerisk verdi som angir sannsynligheten for at en melding som inneholder et blokkert uttrykk, er spam. En høy vektkoeffisient angir stor sannsynlighet for at meldingen som inneholder det blokkerte uttrykket, er spam.

Anti-Spam klassifiserer en melding som spam hvis totalsummen av vektkoeffisientene til blokkerte uttrykk i meldingen overgår den angitte grenseverdien.

Status

I **Status**-delen kan du angi om du vil at Anti-Spam skal skanne meldinger etter blokkerte uttrykk:

- **Aktiv**. Anti-Spam skanner meldinger for å se om de inneholder blokkerte uttrykk.
- **Inaktiv**. Anti-Spam skanner ikke meldinger for å se om de inneholder blokkerte uttrykk.

Vinduet Blokkerte avsendere

Knappen

Klikk på denne knappen for å åpne en meny der du kan velge følgende handlinger:

- **Importer og legg til i eksisterende**. Velg dette alternativet hvis du vil importere en liste over blokkerte avsendere fra en CSV-fil. Gjeldende liste over avsendere slettes ikke.
- **Importer og erstatt eksisterende**. Velg dette alternativet hvis du vil importere en liste over blokkerte avsendere fra en CSV-fil. Gjeldende liste over avsendere slettes.
- **Eksporter**. Velg dette alternativet hvis du vil eksportere en liste over blokkerte avsendere til en CSV-fil.

Listen Blokkerte avsendere

Inneholder en liste over adresser som Anti-Spam klassifiserer som spamkilder.

Du kan legge til en adresse eller adressemaske i listen.

Hvis verdien *Aktiv* er angitt på adresselinjen i **Status**-kolonnen, klassifiserer Anti-Spam automatisk adressen som blokkert.

Hvis verdien *Inaktiv* er angitt på adresselinjen i **Status**-kolonnen, fjerner Anti-Spam automatisk denne adressen fra listen.

Avsenderadresse

Denne kolonnen viser e-postadressen eller e-postadressemasken til den blokkerte avsenderen.

Status

Denne kolonnen viser om Anti-Spam klassifiserer meldinger som mottas fra denne adressen, som spam.

Hvis verdien *Aktiv* er angitt på adresselinjen, klassifiserer Anti-Spam meldinger fra denne adressen som spam.

Hvis verdien *Inaktiv* er angitt på adresselinjen, fjerner Anti-Spam den valgte adressen fra listen.

Rediger

Klikk på denne knappen for å åpne et vindu der du kan endre URLen eller URL-masken som er valgt i listen.

Slett

Når du klikker på denne knappen, fjerner Anti-Spam den valgte adressen eller adressemasken fra listen.

Legg til

Klikk på denne knappen for å åpne et vindu der du kan legge til en URL eller en URL-maske i listen.

Vinduet Blokkerte uttrykk

Knappen

Klikk på denne knappen for å åpne en meny der du kan velge følgende handlinger:

- **Importer og legg til i eksisterende**. Velg dette alternativet hvis du vil importere en liste over blokkerte uttrykk fra en CSV-fil. De aktuelle uttrykkene slettes ikke.
- **Importer og erstatt eksisterende**. Velg dette alternativet hvis du vil importere en liste over blokkerte uttrykk fra en CSV-fil. De aktuelle uttrykkene slettes.
- **Eksporter**. Velg dette elementet hvis du vil eksportere en liste over blokkerte uttrykk til en CSV-fil.

Liste over blokkerte uttrykk

Inneholder nøkkeluttrykk, noe som indikerer at meldinger med disse uttrykkene er spam.

Du kan legge til et uttrykk eller en uttrykksmaske i listen.

Hvis verdien *Aktiv* er angitt på uttrykkslinjen i **Status**-kolonnen, bruker Anti-Spam denne adressen ved filtrering av meldinger.

Hvis verdien *Inaktiv* er angitt på uttrykkslinjen i **Status** kolonnen, fjerner Anti-Spam dette uttrykket fra listen, og bruker det ikke ved filtrering av meldinger.

Rediger

Klikk på denne knappen for å åpne et vindu der du kan endre et uttrykk eller en uttrykksmaske som er valgt fra listen.

Slett

Når du klikker på denne knappen, fjerner Anti-Spam det valgte uttrykket eller den valgte uttrykksmasken fra listen.

Legg til

Klikk på denne knappen for å åpne et vindu der du kan legge til et uttrykk eller en uttrykksmaske i listen.

Vinduet Legg til / rediger e-postadresse

Adressemaske for e-post

I dette vinduet kan du angi en e-postadresse eller en e-postadressemaske.

Når du angir en maske, kan du bruke jokertegnene `*` og `?`, der `*` representerer et hvilket som helst tegnkombinasjon og `?` står for et hvilket som helst tegn.

Status

I delen **Status** kan du angi om Anti-Spam skal blokkere meldinger som sendes fra denne adressen, ved skanning av meldinger i henhold til listen over tillatte/blokkerte avsendere.

- **Aktiv**. Anti-Spam blokkerer meldinger som sendes fra denne adressen.
- **Inaktiv**. Anti-Spam blokkerer ikke meldinger som sendes fra denne adressen.

Vinduet Legg til / rediger tillatte uttrykk

Uttrykksmaske

Et uttrykk eller en uttrykksmaske som indikerer at meldingen ikke er spam.

Vektkoeffisient for uttrykk

En numerisk verdi som angir sannsynligheten for at en melding som inneholder et tillatt uttrykk, ikke er spam. En høy vektkoeffisient angir stor sannsynlighet for at meldingen som inneholder det tillatte uttrykket, ikke er spam.

Anti-Spam vil ikke klassifisere en melding som spam hvis totalsummen av vektkoeffisientene til tillatte uttrykk i meldingen overgår den angitte grenseverdien.

Status

I delen **Status** kan du angi om Anti-Spam skal skanne meldinger for å se om de inneholder et bestemt tillatt uttrykk.

- **Aktiv**. Anti-Spam skanner meldinger for å se om de inneholder det tillatte uttrykket.
- **Inaktiv**. Anti-Spam skanner ikke meldinger for å se om de inneholder det tillatte uttrykket.

Vinduet Tillatte avsendere

Knappen

Klikk på denne knappen for å åpne en meny der du kan velge følgende handlinger:

- **Importer og legg til i eksisterende**. Velg dette alternativet hvis du vil importere en liste over tillatte avsendere fra en CSV-fil. Gjeldende liste over avsendere slettes ikke.
- **Importer og erstatt eksisterende**. Velg dette alternativet hvis du vil importere en liste over tillatte avsendere fra en CSV-fil. Gjeldende liste over avsendere slettes.
- **Eksporter**. Velg dette alternativet hvis du vil eksportere en liste over tillatte avsendere til en CSV-fil.

Listen Tillatte avsendere

Inneholder en liste over avsenderadresser. Meldinger fra disse adressene klassifiseres som nyttig (ikke spam).

Du kan legge til en adresse eller adressemaske i listen.

Hvis verdien *Aktiv* er angitt på adresselinjen i **Status**-kolonnen, klassifiserer Anti-Spam alle meldinger fra denne avsenderen som nyttige.

Hvis verdien *Inaktiv* er angitt på adresselinjen i **Status**-kolonnen, klassifiserer ikke Anti-Spam alle meldinger fra denne avsenderen som nyttige, og skanner dem ved hjelp av standard skannemetoder.

Avsenderadresse

Denne kolonnen viser e-postadressen eller e-postadressemasken til den tillatte avsenderen.

Status

Denne kolonnen viser om Anti-Spam klassifiserer meldinger som mottas fra denne adressen, som nyttig (ikke spam).

Hvis verdien *Aktiv* er angitt på adresselinjen, klassifiserer Anti-Spam meldinger fra denne adressen som nyttig.

Hvis verdien *Inaktiv* er angitt på adresselinjen, fjerner Anti-Spam den valgte adressen fra listen.

Rediger

Klikk på denne knappen for å åpne et vindu der du kan endre en URL eller en URL-maske på listen over tillatte avsendere.

Slett

Når du klikker på denne knappen, fjerner Anti-Spam den valgte adressen eller adressemasken fra listen.

Legg til

Klikk på denne knappen for å åpne et vindu der du kan legge til en URL eller en URL-maske på listen over tillatte avsendere.

Legg til mottakere av e-postene mine som tillatte avsendere

Hvis avkrysningsboksen er valgt, legger programmet e-postmottakere til i listen over tillatte avsendere.

Vinduet Tillatte uttrykk

Knappen

Klikk på denne knappen for å åpne en meny der du kan velge følgende handlinger:

- **Importer og legg til i eksisterende**. Velg dette alternativet hvis du vil importere en liste over tillatte uttrykk fra en CSV-fil. De aktuelle uttrykkene slettes ikke.
- **Importer og erstatt eksisterende**. Velg dette alternativet hvis du vil importere en liste over tillatte uttrykk fra en CSV-fil. De aktuelle uttrykkene slettes.
- **Eksporter**. Velg dette alternativet hvis du vil eksportere en liste over tillatte uttrykk til en CSV-fil.

Liste over tillatte uttrykk

Inneholder viktige uttrykk. Hvis disse uttrykkene oppdages i en melding, angir de at meldingen ikke er spam.

Du kan legge til et uttrykk eller en uttrykksmaske i listen.

Hvis verdien *Aktiv* er angitt på uttrykkslinjen i **Status**-kolonnen, bruker Anti-Spam denne adressen ved filtrering av meldinger.

Hvis verdien *Inaktiv* er angitt på uttrykkslinjen i **Status**-kolonnen, brukes ikke dette uttrykket når Anti-Spam filtrerer meldinger.

Rediger

Når du klikker på denne knappen, åpnes et vindu der du kan endre et uttrykk eller en uttrykksmaske som er valgt fra listen.

Slett

Når du klikker på denne knappen, fjerner Anti-Spam det valgte uttrykket eller den valgte uttrykksmasken fra listen.

Legg til

Når du klikker på denne knappen, åpnes et vindu der du kan legge til et uttrykk eller en uttrykksmaske i listen.

Innstillinger for Safe Money

Aktiver/deaktiver Safe Money

Denne bryteren aktiverer/deaktiverer Safe Money.

Hvis knappen er grønn, overvåker programmet alle forsøk på å få tilgang til nettstedene til banker eller betalingssystemer, og utfører standardhandlingen som er angitt av brukeren. Som standard blir brukeren bedt om å bekrefte start av Beskyttet nettleser når programmet kjører i modusen Safe Money.

Hvis knappen er rød, tillater programmet besøk på nettstedene til banker eller betalingssystemer ved hjelp av standard nettleser.

Finn ut mer

Ved å klikke på denne koblingen åpner du en side med komponentdetaljer i et nettleservindu.

I **Ved første tilgang til nettstedet til banker eller betalingssystemer** kan du velge handlingen som programmet skal utføre den første gangen du besøker disse nettstedene.

Kjør Beskyttet nettleser

Hvis programmet oppdager et forsøk på å få tilgang til det angitte nettstedet, åpnes nettstedet i Beskyttet nettleser. Standardleseren som brukes for å få tilgang til nettstedet, viser en melding som informerer deg om at Beskyttet nettleser startes.

Spør brukeren

Hvis programmet oppdager et forsøk på å få tilgang til det angitte nettstedet, blir du bedt om å starte Beskyttet nettleser eller åpne nettstedet i standardleseren.

Ikke kjør Beskyttet nettleser

Når du prøver å åpne det angitte nettstedet, vil ikke programmet bruke Beskyttet nettleser. Nettstedet åpnes i en standard nettleser.

I delen **Ekstra** kan du konfigurere flere innstillinger for Safe Money.

Hvis du vil fortsette til nettstedet fra vinduet Safe Money, bruker du Standard nettleser

Fra rullegardinlisten kan du velge nettleseren som programmet skal bruke til å åpne nettstedene til banker og betalingssystemer som er valgt i vinduet til Safe Money.

Safe Money er tilgjengelig for brukere av følgende nettlesere: Microsoft Internet Explorer, Microsoft Edge basert på Chromium, Mozilla Firefox, Google Chrome og Yandex.Browser.

Som standard bruker Safe Money nettleseren som er standard nettleser i operativsystemet.

Opprett snarvei for Safe Money

Klikk på denne lenken for å opprette en snarvei for start av Safe Money. Denne snarveien åpner et vindu med en liste over nettstedene til banker og betalingssystemer, som krever tilgang via Beskyttet nettleser.

På 64-biters versjoner av Windows 8, Windows 8.1 og Windows 10 brukes virtualisering av maskinvare for å beskytte nettleseren.

Innstillinger for Sikker surfing

Innstillinger	Beskrivelse
Sikkerhetsnivå	Programmet bruker ulike grupper med innstillinger for å kjøre Sikker surfing. Innstillingene som er lagret i programmet, kalles *sikkerhetsnivåer*. • **Ekstremt**. Sikkerhetsnivået for nettrafikk som Sikker surfing bruker ved grundig skanning av nettrafikk som mottas av datamaskinen over HTTP- og FTP-protokollene. Sikker surfing kjører en detaljert skanning av alle nettrafikkobjekter ved å bruke det fullstendige settet med programdatabaser. Komponenten utfører også den dypeste heuristiske analysen. • **Optimalt**. Sikkerhetsnivået for nettrafikk som oppnår den optimale balansen mellom ytelse for Kaspersky-programmet og nettrafikksikkerhet. Sikker surfing utfører en heuristisk analyse på middels nivå. Dette sikkerhetsnivået for nettrafikk anbefales av Kaspersky-spesialister. • **Lavt**. Sikkerhetsnivået for nettrafikk som har innstillinger som sikrer maksimal skannehastighet for nettrafikk. Sikker surfing utfører en heuristisk analyse på lavt nivå.
Handling ved oppdagelse av trussel	• **Varsle**. Sikker surfing informerer deg når det oppdages infiserte eller potensielt infiserte objekter, og ber deg om å velge ytterligere handlinger for de aktuelle objektene. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er deaktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**. • **Utfør handling automatisk**. Sikker surfing velger automatisk en handling ut fra gjeldende innstillinger. Hvis en webressurs er oppført blant unntakene, eller hvis den ikke inneholder infiserte eller potensielt infiserte objekter, vil Sikker surfing tillate tilgang til denne ressursen. Hvis et skann av Sikker surfing oppdager et infisert eller potensielt infisert objekt i webressursen, blokkeres tilgang til den aktuelle ressursen. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er valgt under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**. • **Blokker nedlasting**. Hvis du velger dette alternativet og et infisert objekt oppdages i nettrafikk, blokkerer Sikker surfing tilgangen til dette objektet og viser en melding i nettleseren.
Skannemetoder **Sjekk nettadressen mot databasen over skadelig programvare**	Ved å skanne koblingene for å finne ut om de er inkludert i databasen over skadelige koblinger, kan du spore nettsteder som er lagt til i Avslå-listen. Databasen over skadelige koblinger opprettes av Kasperskys eksperter. Det utgjør en del av programvaredistribusjonssettet, og det oppdateres sammen med Kaspersky-programmets database.
Sjekk nettadressen mot databasen over adresser som inneholder annonseprogrammer	Ett eksempel kan være programvare som omdirigerer søket ditt på Internett til et annonseringsnettsted. På denne måten kommer du til et annonseringsnettsted i stedet for nettressursen som er mest relevant for søket ditt.
Sjekk URL mot	Et eksempel på denne kategorien kan være et fjernstyringsverktøy som brukes

databasen over URL-er som inneholder legitime programmer som kriminelle kan bruke til å skade datamaskinen eller personlige data	lovlig til feilsøking av systemadministratorer. En kriminell kan installere et slikt verktøy på datamaskinen din uten at du vet om det for å få tilgang til datamaskinen din og bruke den til kriminelle formål. Kaspersky-programmet tillater nedlasting av slike programmer ved å klikke på lenker på nettsider. Engangskoblinger er et unntak. Du kan ikke bruke dem til å laste ned legitime programmer som hackere kan bruke til å skade datamaskinen eller dataene dine.
Bruk heuristisk analyse	En teknikk for å oppdage trusler som ikke kan identifiseres ved å bruke den gjeldende versjonen av programdatabasene til Kaspersky. Den lar deg finne filer som kan inneholde ukjent skadelig programvare eller en ny modifisering av kjent skadelig programvare. Når nettrafikken skannes etter virus og andre programmer som utgjør en trussel, utfører den heuristiske analysen instruksjoner i de kjørbare filene. Antall instruksjoner som utføres av den heuristiske analysen, avhenger av nivået som er angitt for den heuristiske analysen. Det heuristiske analysenivået angir balansen mellom grundighetsnivået på søket etter nye trusler, belastningen på operativsystemets ressurser og tiden som kreves for den heuristiske analysen.
Anti-Phishing **Sjekk nettadressen mot databasen over phishing- og falske kryptoadresser** (i noen abonnementsplaner **Sjekk nettadressen mot databasen over phishing-adresser**)	Innholdet i databasen med phishing-koblinger og falske kryptobørser inkluderer nettadressene til aktuelle kjente nettsteder som brukes til phishing-angrep. Kaspersky supplerer denne databasen med adresser som hentes fra den internasjonale organisasjonen Anti-Phishing Working Group. Databasen med phishing-koblinger og skjemaer på falske kryptobørser er en del av programvaredistribusjonssettet, og den oppdateres sammen med Kaspersky-programmets database.
Bruk heuristisk analyse	En teknikk for å oppdage trusler som ikke kan identifiseres ved å bruke den gjeldende versjonen av programdatabasene til Kaspersky. Dette gjør det mulig å oppdage phishing, selv om nettadressen ikke er i databasen over phishing-nettsteder.
Kontroller URLer	Komponenten URL-veileder kontrollerer lenken på nettsider som åpnes i Chromium-basert Microsoft Edge, Google Chrome og Mozilla Firefox. Kaspersky-programmet viser ett av følgende ikoner ved siden av hver kobling som er kontrollert:  – hvis det lenkede nettstedet er sikkert ifølge Kaspersky  – hvis det ikke finnes informasjon om sikkerhetsstatusen til den koblede websiden  – hvis Kaspersky mener at hackere kan forårsake skade på datamaskinen din eller dataene dine hvis du bruker nettsiden som koblingen åpner  – vis Kaspersky mener at nettsiden som koblingen åpner kan være infisert eller hacket  – hvis det lenkede nettstedet er farlig ifølge Kaspersky Hvis du vil vise et popup-vindu med mer informasjon om koblingen, peker du på det tilhørende ikonet.
På alle nettsteder unntatt de som er angitt **Behandle unntak**	Når dette alternativet er valgt, skanner programmet koblinger på alle nettsteder, bortsett fra de som er angitt i vinduet **Unntak**. Vinduet **Unntak** åpnes når du klikker på koblingen **Behandle unntak**.
Kun på angitte	Når dette alternativet er valgt, skanner Kaspersky kun koblinger på nettsteder

nettsteder **Konfigurer kontrollerte nettsteder**	som er angitt i vinduet **Kontrollerte nettsteder**. Vinduet **Kontrollerte nettsteder** åpnes når du klikker på koblingen **Konfigurer kontrollerte nettsteder**.
Konfigurer URL-veileder	• **Alle URLer**. Programmet skanner koblinger for alle typer nettsider. • **Kun URLer i søkeresultater**. Programmet skanner koblinger for nettsider som inneholder søkeresultater mottatt fra søkemotorer.
Nettstedkategorier	Hvis avmerkingsboksen **Vis informasjon i kategoriene til nettsteder** er aktivert, legger programmet til koblingskommentarer for å angi om nettsiden tilhører en av de indikerte kategoriene (for eksempel, **Vold** eller **Vokseninnhold**). Du kan fjerne avmerkingsboksene ved siden av kategoriene som ikke krever advarsler.
Ikke skann trafikk fra klarerte URLer	Hvis avmerkingsboksen er aktivert, skanner ikke Sikker surfing innholdet på nettsider/nettsteder som har adresser inkludert i listen over klarerte nettadresser. Du kan legge til både spesifikke nettside-/nettstedsadresser samt adressemasker for nettsider/nettsteder i listen over klarerte nettadresser. Listen over klarerte nettadresser er tilgjengelig i vinduet **Klarerte URLer**, som kan åpnes ved å klikke på koblingen fra **klarerte URLer**.

Vinduet Nettstedene til Kaspersky og deres partnere

Dette vinduet viser en liste over nettstedene til Kaspersky og deres partnere.

Denne listen er kompilert og oppdatert av Kasperskys eksperter. Listen oppdateres automatisk når databaser og programmoduler oppdateres.

Innstillinger for Nettverkangrepsblokkering

Nettverkangrepsblokkering lastes inn når du starter operativsystemet, og skanner innkommende nettverkstrafikk etter aktiviteter som har de samme egenskapene som nettverksangrep. Når Kaspersky-programmet oppdager forsøk på nettverksangrep på en brukers datamaskin, blokkeres nettverkstilkoblingen til den angripende datamaskinen. Beskrivelser av kjente typer nettverksangrep og metoder for å nøytralisere dem er spesifisert i databasene til Kaspersky-programmet. Listen over nettverksangrep som kan oppdages av Nettverkangrepsblokkering, oppdateres når programdatabasene og modulene oppdateres.

Innstillinger for Nettverkangrepsblokkering

Innstillinger	Beskrivelse
Behandle portskanning og flooding som angrep	*Flooding* er et angrep på organisasjonens nettverksressurser (f.eks. webservere). Dette angrepet består av å sende en massiv mengde trafikk for å oppta trafikkapasiteten på et nettverk. Som et resultat av dette, får ikke brukerne tilgang til organisasjonens nettverksressurser. *Portskanningangrep* består av å skanne UDP- og TCP-porter, samt nettverkstjenester på datamaskinen. Dette angrepet kan fastslå datamaskinens sårbarhetsnivå før flere farlige typer nettverksangrep skjer. Portskanning gjør også at hackere kan fastslå datamaskinens operativsystem og velge spesifikke angrep for det. Hvis bryteren er på, vil Nettverkangrepsblokkering blokkere portskanning og flooding.
Legg til den angripende datamaskinen i listen over blokkerte datamaskiner i N min	Hvis bryteren er på, legger Nettverkangrepsblokkering til den angripende datamaskinen i blokkeringslisten. Dette betyr at Nettverksangrepsblokkering blokkerer nettverkstilkoblingen til den angripende datamaskinen etter det første angrepsforsøket i lden angitte tidsperioden for å automatisk beskytte brukerens datamaskin mot eventuelle fremtidige nettverksangrep fra samme adresse. Den angripende datamaskinen kan legges til i blokkeringslisten med en minstetid på ett minutt. Maksimal varighet er 32 768 minutter.
Behandle unntak	Listen inneholder IP-adresser som Nettverkangrepsblokkering ikke blokkerer nettverksangrep fra. Programmet rapporterer ikke informasjon om nettverksangrep fra IP-adresser som er inkludert i unntakslisten.

Innstillinger for Inntrengningsbeskyttelse

Aktiver/deaktiver Inntrengningsbeskyttelse

Denne bryteren aktiverer/deaktiverer Inntrengningsbeskyttelse.

Finn ut mer

Ved å klikke på denne koblingen åpner du en side med komponentdetaljer i et nettleservindu.

Klarer programmer med digital signatur

Hvis dette alternativet er aktivert, klassifiserer Inntrengningsbeskyttelse programmer med digital signatur som klarerte. Inntrengningsbeskyttelse flytter disse programmene til gruppen **Klarert** og vil ikke skanne disse programmenes aktivitet.

Hvis alternativet er deaktivert, klassifiserer ikke Inntrengningsbeskyttelse programmer med digitale signaturer som klarerte, og skanner deres aktiviteter. Inntrengningsbeskyttelse klassifiserer programmene til klarerte programvareleverandører (for eksempel Microsoft) som klarerte, uavhengig av hvorvidt avkrysningsboksen er valgt.

Last inn regler for programmer fra Kaspersky Security Network (KSN)

Hvis denne boksen er avmerket, sender Inntrengningsbeskyttelse en forespørsel til Kaspersky Security Network-databasen for å kunne definere programgruppen.

Hvis denne boksen ikke er merket av, vil ikke Inntrengningsbeskyttelse søke etter informasjon i Kaspersky Security Network-databasen for å definere programmets klareringsgruppe.

Klareringsgruppe for programmer som ikke kunne legges til eksisterende grupper

Ved å klikke på denne lenken åpnes vinduet **Klareringsgruppe for programmer som ikke kunne legges til eksisterende grupper**. I dette vinduet kan du velge hvilken klareringsgruppe ukjente programmer skal tilordnes.

Du kan velge ett av følgende alternativer:

- Klarert
- Lavt begrenset
- Høyt begrenset
- Uklarert

Klareringsgruppe for programmer startet før oppstart av <PRODUCT>

Ved å klikke på denne lenken åpnes vinduet **Klareringsgruppe for programmer startet før oppstart av <PRODUCT>**. I dette vinduet kan du endre klareringsgruppen for programmer som startes før oppstart av Kaspersky. Som standard begrenses nettverksaktivitetene til programmer som startes før Kaspersky, i henhold til reglene i den valgte klareringsgruppen.

Som standard tilordnes programmer som startes før oppstart av Kaspersky, til en av klareringsgruppene i henhold til reglene som er opprettet av Kaspersky.

Behandle programmer

Ved å klikke på denne lenken åpnes vinduet **Behandle programmer**. I dette vinduet kan du redigere listen over programregler.

Behandle ressurser

Ved å klikke på denne lenken åpnes vinduet **Behandle ressurser**. I dette vinduet kan du opprette en liste over personlige data og en liste over innstillinger og ressurser for operativsystemet. Tilgang til disse elementene kontrolleres av Inntrengningsbeskyttelse.

Vinduet Websignaler

Dette vinduet viser en liste over websignaler.

Denne listen er kompilert og oppdatert av Kasperskys eksperter. Listen oppdateres automatisk når databaser og programmoduler oppdateres.

Kategorier og unntak for Privat surfing

Webanalysetjenester

Hvis alternativet er aktivert, blokkerer komponenten Privat surfing webanalysetjenester som bruker sporing av aktiviteter til å analyse nettaktivitetene dine.

Klikk på koblingen **Vis liste** for å åpne et vindu med en liste over webanalysetjenester som bruker aktivitetssporing til å spore nettaktivitetene dine.

Reklamebyråer

Hvis alternativet er aktivert, blokkerer Privat surfing sporing av nettaktivitetene dine for reklamebyråer, som bruker dem til reklame formål.

Klikk på koblingen **Vis liste** for å åpne et vindu med en liste over reklamebyråer som sporer nettaktivitetene dine for reklameformål.

Websignaler

Hvis alternativet er aktivert, blokkerer Privat surfing sporing av dine nettaktiviteter ved hjelp av websignaler. Websignaler er objekter som er innebygd i websider, men er usynlige for brukere.

Klikk på koblingen **Vis liste** for å åpne et vindu med en liste over websignaler.

Sosiale nettverk

Hvis alternativet er aktivert, vil komponenten Privat surfing blokkere forsøk på innsamling av data når du besøker sosiale nettverk, unntatt innsamling av data utført av disse sosiale nettverkene. Blokkering av datainnsamling lar deg fortsatt bruke «Lik», «+1» og lignende funksjoner.

Merk av i avmerkingsboksene med navnene på sosiale nettverk for å angi hvilke sosiale nettverk du vil blokkere datainnsamling på.

Unntak

Når du klikker på denne koblingen, åpnes et vindu er du kan angi nettstedene der du vil tillate sporing av nettaktiviteter.

Vinduet Inkompatible nettsteder

Dette vinduet viser en liste over nettsteder som kan slutte å fungere hvis du blokkerer innsamling av data, i henhold til informasjonen Kaspersky har tilgjengelig.

Denne listen er kompilert og oppdatert av Kasperskys eksperter. Listen oppdateres automatisk når databaser og programmoduler oppdateres.

Vinduet Innstillinger for Privat surfing

Aktiver/deaktiver Privat surfing

Hvis vekselbryteren er slått på, og du er koblet til Internett oppdager komponenten Privat surfing sporingstjenesters forsøk på innsamling av data. Sporingstjenester bruker informasjonen som mottas til å analysere aktivitetene dine, og de kan bruke analyseresultatene til å vise deg relevant reklame.

Kun innhente statistikk

Når dette alternativet er valgt, kjører komponenten Privat surfing i *oppdagelsesmodus*, og lar deg vise rapporter om oppdagede forsøk på innsamling av data.

Blokker innsamling av data

Når dette alternativet er valgt, vil komponenten Privat surfing fungere i *blokkeringsmodus*, og oppdage og blokkere forsøk på innsamling av data. Informasjon om disse forsøkene skrives i en rapport.

Kategorier og unntak

Klikk på denne koblingen for å åpne et vindu der du kan angi kategoriene til sporingstjenester du ønsker å blokkere eller tillate innsamling av data for. Fra dette vinduet kan du opprette en liste over nettsteder der du vil tillate sporing.

Blokker sporing

Hvis boksen er valgt og blokkeringsmodus er aktivert når du besøker et nettsted, sender nettleseren HTTP-overskriften «Ikke spor» til nettstedet. Da tillates ikke sporing av aktivitetene dine.

Tillat innsamling av data på nettstedene til Kaspersky og deres partnere

Hvis alternativet er aktivert, vil Kaspersky tillate datainnsamling på nettstedene til Kaspersky og deres partnere.

Nettstedene til Kaspersky og deres partnere

Klikk på denne koblingen for å åpne et vindu med en liste over nettstedene til Kaspersky og deres partnere.

Tillat innsamling av data på inkompatible nettsteder

Hvis alternativet er aktivert, vil Kaspersky tillate datainnsamling på nettsteder som kan slutte å fungere på grunn av slik blokkering.

Inkompatible nettsteder

Klikke på denne koblingen for å åpne et vindu med en liste over nettsteder som kan slutte å fungere hvis datainnsamling er blokkert.

Vinduet Reklamebyråer

Dette vinduet viser en liste over reklamebyråer som sporer nettaktivitetene dine for reklameformål.

Denne listen er kompilert og oppdatert av Kasperskys eksperter. Listen oppdateres automatisk når databaser og programmoduler oppdateres.

Vinduet Webanalysetjenester

Dette vinduet viser en liste over webanalysetjenester som bruker aktivitetssporing til å analysere nettaktivitetene dine.

Denne listen er kompilert og oppdatert av Kasperskys eksperter. Listen oppdateres automatisk når databaser og programmoduler oppdateres.

Innstillinger for E-post-Antivirus

Innstillinger	Beskrivelse
Sikkerhetsnivå	Kaspersky-programmet bruker forskjellige innstillingsgrupper for å kjøre E-post-Antivirus. Innstillingene som er lagret i programmet, kalles *sikkerhetsnivåer*. • **Ekstremt**. Hvis dette e-postsikkerhetsnivået er valgt, bruker E-post-Antivirus den strengeste kontrollen på e-postmeldinger. E-post Antivirus skanner innkommende og utgående e-postmeldinger. Den utfører også en dyp heuristisk analyse. E-postsikkerhetsnivået Høyt bør brukes når du arbeider i et farlig miljø. Et slikt miljø kan for eksempel være tilkobling til en gratis e-posttjeneste fra et nettverk som ikke overvåkes av en sentralisert e-postbeskyttelse. • **Optimalt**. E-postsikkerhetsnivået som oppnår den optimale balansen mellom ytelse for Kaspersky-programmet og e-postsikkerhet. E-post Anti-Virus skanner innkommende og utgående e-postmeldinger. Den utfører også en heuristisk analyse på middels nivå. Dette e-postsikkerhetsnivået anbefales av Kasperskys eksperter. • **Lavt**. Dette er e-postsikkerhetsnivået som E-post Antivirus kun bruker for å skanne innkommende e-postmeldinger, samt for å utføre en overflateheuristisk analyse. Komponenten bruker ikke dette nivået til å skanne arkiver som er knyttet til meldinger. Når dette e-postsikkerhetsnivået er valgt, skanner E-post Antivirus e-postmeldinger så raskt som mulig og bruker minst mulig ressurser i operativsystemet. E-postsikkerhetsnivået Lavt kan brukes når du arbeider i et godt beskyttet miljø. Et slikt miljø kan for eksempel være et lokalt nettverk som bruker sentralisert e-postbeskyttelse.
Handling ved oppdagelse av trussel	• **Spør brukeren**. E-post-Antivirus informerer deg når det oppdages infiserte eller potensielt infiserte objekter, og ber deg om å velge ytterligere handlinger for de aktuelle objektene. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er deaktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**. • **Velg handling automatisk**. Når det oppdages infiserte eller potensielt infiserte objekter, utfører E-post-Antivirus automatisk handlingene som er anbefalt av Kasperskys eksperter. For infiserte objekter, er denne handlingen Desinfiser. Denne verdien blir valgt som standard. Før et infisert objekt desinfiseres eller slettes, vil E-post-Antivirus opprette sikkerhetskopier, slik at objektet kan gjenopprettes eller desinfiseres på et senere tidspunkt om nødvendig. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er valgt under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**. • **Desinfiser, slett hvis desinfisering ikke er mulig**. Hvis et infisert objekt blir oppdaget i en innkommende eller utgående melding, prøver Kaspersky-programmet å desinfisere det oppdagede objektet. Brukeren kan få tilgang til meldingen med et sikkert vedlegg. Hvis Kaspersky-programmet ikke klarer å desinfisere objektet, slettes det. Kaspersky-programmet legger til informasjon om den utførte handlingen i meldingens emne: *[Melding behandlet] <meldingens emne>*. • **Desinfiser, blokker hvis desinfisering ikke er mulig**. Hvis et infisert objekt oppdages i en innkommende melding, prøver Kaspersky-programmet å desinfisere det oppdagede objektet. Brukeren kan få tilgang til meldingen med et

	sikkert vedlegg. Hvis objektet ikke kan desinfiseres, legger Kaspersky-programmet til en advarsel i meldingens emne: [Melding infisert] <meldingens emne>. Brukeren vil ha tilgang til meldingen med det originale vedlegget. Hvis et infisert objekt oppdages i en utgående melding, prøver Kaspersky-programmet å desinfisere det oppdagede objektet. Hvis Kaspersky-programmet ikke kan desinfisere objektet, blokkeres sending av meldingen, og en feilmelding vises i e-postklienten. • **Blokker**. Hvis et infisert objekt oppdages i en innkommende melding, legger Kaspersky-programmet til en advarsel i meldingens emne: Brukeren vil ha tilgang til meldingen med det originale vedlegget. Hvis et infisert objekt oppdages i en utgående melding, blokkerer Kaspersky-programmet sending av meldingen, og e-postklienten viser en feilmelding.
Beskyttelsesomfang	*Beskyttelsesomfanget* inkluderer objekter som komponenten skal sjekke når den kjøres: Innkommende og utgående meldinger eller Bare innkommende meldinger. Du trenger bare å skanne innkommende meldinger for å beskytte datamaskinene dine. Du kan slå på skanning av utgående meldinger for å forhindre at infiserte filer blir sendt i arkiver. Du kan også slå på skanning av utgående meldinger hvis du vil forhindre at filer i bestemte formater sendes, for eksempel lyd- og videofiler.
Skann trafikk over POP3, SMTP, NNTP og IMAP	Denne avmerkingsboksen aktiverer/deaktiverer skanning av e-posttrafikk som sendes over POP3-, SMTP-, NNTP- og IMAP-protokollene, med E-post Antivirus.
Koble til utvidelsen for Microsoft Outlook	Hvis avmerkingsboksen er merket av, skannes e-postmeldinger som sendes over POP3-, SMTP-, NNTP- og IMAP-protokollene ved bruk av en utvidelse som er integrert i Microsoft Outlook. Hvis e-post skannes ved bruk av utvidelsen for Microsoft Outlook, anbefales det å bruke Bufret Exchange-modus. Du kan finne mer informasjon om Bufret Exchange-modus og anbefalinger om hvordan du bruker modusen, i Microsoft Knowledge Base.
Heuristisk analyse	En teknikk for å oppdage trusler som ikke kan identifiseres ved å bruke den gjeldende versjonen av programdatabasene til Kaspersky. Den lar deg finne filer som kan inneholde ukjent skadelig programvare eller en ny modifisering av kjent skadelig programvare. Når du skanner filer etter skadelig kode, utfører den heuristiske analysen instruksjoner i de kjørbare filene. Antall instruksjoner som utføres av den heuristiske analysen, avhenger av nivået som er angitt for den heuristiske analysen. Det heuristiske analysenivået angir balansen mellom grundighetsnivået på søket etter nye trusler, belastningen på operativsystemets ressurser og tiden som kreves for den heuristiske analysen.
Skann vedlagte filer Microsoft Office-formater	Skanner Microsoft Office-filer (DOC, DOCX, XLS, PPT og andre Microsoft-filtyper). Microsoft Office-filer inkluderer også OLE-objekter.
Skann vedlagte arkiver	Skann ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE og andre arkiver. Programmet skanner arkiver ikke bare etter utvidelsene, men også etter formatene deres.
Ikke skann arkiver som er større enn	Hvis avmerkingsboksen er aktivert, utelukker E-post-Antivirus arkiver som er vedlagt i e-postmeldinger, fra skanningen, hvis størrelsen overgår verdien du har angitt. Hvis avmerkingsboksen er deaktivert, skanner E-post Antivirus arkiver av alle størrelser, som er vedlagt i e-postmeldinger.
Begrens tiden for kontroll av arkiver til	Hvis avmerkingsboksen er aktivert, er tidsperioden som kreves for å skanne arkiver som er vedlagt i e-postmeldinger, begrenset til den angitte perioden.

Vedleggsfilter	Vedleggsfilteret fungerer ikke for utgående e-postmeldinger. **Deaktiver filtrering**. Hvis du velger dette alternativet, filtrerer ikke E-post-Antivirus filer som er vedlagt i e-postmeldinger. **Gi nytt navn til utvalgte typer vedlegg**. Hvis du velger dette alternativet, erstatter E-post-Antivirus det siste tegnet i filtypen for vedlagte filer av utvalgte typer, med understrekningstegnet (for eksempel attachment.doc_). Dermed må brukeren gi filen et nytt navn for å åpne den. **Slett utvalgte typer vedlegg**. Hvis du velger dette alternativet, sletter E-post-Antivirus filer av de angitte filtypene som legges ved i e-postmeldinger. Du kan spesifisere typer vedlagte filer som du må omdøpe eller slette fra e-postmeldinger i filmakselisten.

Vinduet Nettverksegenskaper (adapter)

Navn

Navnet på nettverkskortet.

Tilkoblingstype

Type nettverkskort, f.eks. Ethernet, trådløst nettverk eller modemforbindelse.

Status

Nettverksforbindelsens nåværende status, enten *Tilkoblet* eller *Frakoblet*.

I delen **Nye tilkoblinger** kan du velge hvilken handling brannmuren skal utføre når den oppdager en ny forbindelse med dette nettverkskortet.

Be om gruppe

Hvis brannmuren oppdager en ny nettverkstilkobling, varsles du om dette. Du blir også bedt om å velge status for det nye nettverket.

Flytt automatisk nye nettverk til gruppen

Hvis brannmuren oppdager en ny nettverkstilkobling, tilordnes nettverket automatisk statusen som er valgt i rullegardinlisten.

I rullegardinlisten kan du velge en nettverksstatus som Brannmur automatisk skal tilordne nye nettverk.

Innstillinger for Systemvakt

Aktiver/deaktiver

Denne bryteren aktiverer/deaktiverer System Watcher.

Hvis knappen er grønn, vil Systemvakt samle inn og lagre data for alle hendelser i operativsystemet (for eksempel endring av filer, endring av registernøkler, oppstart av drivere, forsøk på å slå av maskinen). Disse dataene brukes til å spore skadelig aktivitet og annen aktivitet i programmet (inkludert løsepengevirus) og til å gjenopprette tilstanden til operativsystemet slik det var før programmet ble installert (for å tilbakestille konsekvensene av skadelig programvare eller annen aktivitet i programmet). I noen tilfeller kan programaktivitet ikke rulles tilbake, for eksempel når et program ble oppdaget av komponenten Inntrengningsbeskyttelse.

Systemvakt samler inn data fra forskjellige kilder, deriblant fra andre komponenter i Kaspersky. Systemvakt analyserer programaktivitet og gir den innhentede informasjonen videre til de andre komponentene i Kaspersky.

I delen **Utnyttelsesbeskyttelse** kan du konfigurere hvilke handlinger som programmet skal utføre når kjørbare filer kjøres av sårbare programmer.

Overvåk forsøk på å utføre uautoriserte operasjoner

Med dette alternativet kan du aktivere/deaktivere Forebygging av utnyttelse.

Hvis dette alternativet er aktivert, sporer Kaspersky kjørbare filer som kjøres av sårbare programmer. Hvis Kaspersky oppdager forsøk på å kjøre en kjørbar fil fra et sårbart program som ikke er startet av brukeren, vil programmet automatisk utføre handlingen som er valgt fra rullegardinlisten **Ved oppdagelse av trussel**.

Ved oppdagelse av trussel

I rullegardinlisten kan du velge handlingen som Systemvakt skal utføre når en kjørbar fil kjøres fra et overvåket sårbart program.

Du kan velge følgende handlinger fra listen:

- **Spør brukeren**. Systemvakt ber brukeren om å angi en handling. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er deaktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**.
- **Velg handling automatisk**. Systemvakt utfører automatisk handlingen som er valgt i Kaspersky-innstillingene, og legger til informasjon om den valgte handlingen i rapporten. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er valgt under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**.
- **Tillat handling**. Systemvakt tillater at den kjørbare filen kjøres.
- **Blokker handling**. Systemvakt blokkerer kjøring av den kjørbare filen.

Handling ved oppdagelse av skadelig programaktivitet eller andre aktiviteter

I rullegardinlisten kan du velge handlingen som Systemvakt skal utføre når skadelig eller annen programaktivitet oppdages basert på analysen av programaktiviteter.

- **Spør brukeren**. Systemvakt ber brukeren om å angi en handling. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er deaktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**.
- **Velg handling automatisk**. Systemvakt utfører handlingen som anbefales av Kasperskys eksperter automatisk. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er valgt under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**.
- **Slett programmet**. Systemvakt sletter programmet.
- **Avslutt programmet**. Systemvakt avslutter alle programmets prosesser.
- **Avslutt programmet**. Systemvakt utfører ingen handlinger på programmet.

Handling som skal utføres hvis skadelig programvare eller andre aktiviteter kan tilbakerulles

I denne rullegardinlisten kan du velge handlingen som Systemvakt skal utføre når det er mulig å rulle tilbake endringer gjort av skadelgi eller annen programaktivitet.

- **Spør brukeren**. Hvis Systemvakt, Fil-Antivirus eller resultatene av en skanneoppgave bekrefter at det er nødvendig med tilbakestilling, vil Systemvakt be brukeren om å velge en handling. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er deaktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**.
- **Velg handling automatisk**. Hvis Systemvakt analyserer aktivitetene til et program og anser dem som skadelige, vil det tilbakestille programmets handlinger og varsle brukeren om denne hendelsen. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er valgt under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**.
- **Rull tilbake**. Systemvakt ruller tilbake skadelig eller annen aktivitet fra programmet.
- **Ikke rull tilbake**. Systemvakt lagrer informasjon om skadelig eller annen aktivitet, men ruller ikke tilbake programmets handlinger.

I delen **Beskyttelse mot skadelige skjermlåsingsprogrammer** kan du velge handlingene som skal utføres når det oppdages forsøk på skjermlåsing. Skjermlåsingsprogrammer er skadelige programmer som begrenser brukerens handlinger på datamaskinen ved å låse skjermen og tastaturet, eller ved å blokkere tilgang til oppgavelinjen og snarveier. Skjermlåsingsprogrammer kan prøve å innkreve løsepenger for å gjenopprette tilgang til operativsystemet. Ved hjelp av beskyttelse mot skjermlåsingsprogrammer kan du lukke eventuelle skjermlåsingsprogrammer ved å taste inn en spesiell tastekombinasjon.

Oppdag og lukk skjermlåsingsprogrammer

Denne boksen aktiverer/deaktiverer beskyttelse mot skjermlåsingsprogrammer.

Hvis alternativet er aktivert og aktiviteter fra skjermlåsingsprogrammer oppdages, kan du stanse aktivitetene ved å bruke en tastekombinasjon som er angitt i rullegardinlisten under avmerkingsboksen.

Bruk følgende tastekombinasjon til å lukke et skjermlåsingsprogram manuelt

I rullegardinlisten kan du velge en nøkkel eller en tastekombinasjon, som gjør det mulig å finne og slette et skjermlåsingsprogram.

Følgende tastekombinasjon brukes som standard: CTRL+ALT+SHIFT+F4.

Innstillinger for File Anti-Virus

Innstillinger	Beskrivelse
Sikkerhetsnivå	Kaspersky-programmet bruker forskjellige innstillingsgrupper for å kjøre File Anti-Virus. Innstillingene som er lagret i programmet, kalles *sikkerhetsnivåer*. • **Ekstremt**. Når dette filsikkerhetsnivået er valgt, kjører File Anti-Virus den strengeste kontrollen på alle filer som åpnes, lagres og startes. File Anti-Virus skanner alle filtyper på alle datamaskinens harddisker, nettverksstasjoner og flyttbare lagringsmedier. Komponenten skanner også arkiver, installasjonspakker og innebygde OLE-objekter. • **Optimalt**. Dette filsikkerhetsnivået anbefales av Kaspersky Labs eksperter. File Anti-Virus skanner kun angitte filformater på datamaskinens harddisker, nettverksstasjoner og flyttbare lagringsmedier, samt innebygde OLE-objekter. File Anti-Virus skanner ikke arkiver eller installasjonspakker. • **Lavt**. Innstillingene for dette filsikkerhetsnivået sikrer maksimal skannehastighet. File Anti-Virus skanner kun filer med angitte filtyper på alle harddisker, nettverksstasjoner og flyttbare lagringsmedier på datamaskinen. File Anti-Virus skanner ikke sammensatte filer.
Handling ved oppdagelse av trussel	• **Spør brukeren**. File Anti-Virus informerer deg når det oppdages infiserte eller potensielt infiserte objekter, og ber deg om å velge ytterligere handlinger for de aktuelle objektene. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er deaktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**. • **Velg handling automatisk**. File Anti-Virus bruker automatisk handlingen som anbefales av Kasperskys eksperter, når det oppdages infiserte eller potensielt infiserte objekter. For infiserte objekter, er denne handlingen Desinfiser. Denne verdien blir valgt som standard. File Anti-Virus oppretter automatisk en sikkerhetskopi før programmet prøver å desinfisere eller slette et infisert objekt, slik at objektet kan gjenopprettes eller desinfiseres på et senere tidspunkt. Dette alternativet er tilgjengelig hvis alternativet **Utfør anbefalte handlinger automatisk** er valgt under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**. • **Desinfiser, slett hvis desinfisering ikke er mulig**. Hvis du velger denne handlingen, prøver programmet automatisk å desinfisere alle infiserte filer som den finner. Hvis desinfisering ikke er mulig, sletter programmet objektene. • **Desinfiser, blokker hvis desinfisering ikke er mulig**. Hvis du velger denne handlingen, prøver programmet automatisk å desinfisere alle infiserte filer som den finner. Hvis desinfiseringen mislykkes, legger programmet til informasjon om de infiserte filene den finner på listen over detekterte objekter. • **Blokker**. Hvis dette alternativet er valgt, blokkerer File Anti-Virus automatisk alle infiserte filer uten å desinfisere dem. Når du prøver å desinfisere eller slette en infisert fil, oppretter programmet først en sikkerhetskopi i tilfelle du trenger å gjenopprette filen, eller det blir mulig å desinfisere den, senere.

Filtyper	**Alle filer**. Hvis denne innstillingen er aktivert, skanner programmet alle filer uten unntak (alle formater og filtyper). **Filer skannet etter format**. Hvis du velger denne innstillingen, skanner programmet kun potensielt infiserte filer. Før du søker etter skadelig kode i en fil, analyseres filens interne filhode for å fastsette filformatet (TXT, DOC, EXE osv.). Skanningen ser også etter filer med bestemte filtyper. **Filer skannet etter filtype**. Hvis du velger denne innstillingen, skanner programmet kun potensielt infiserte filer. Filformatet gjenkjennes ved hjelp av filtypen.
Rediger beskyttelsesomfang	Ved å klikke på denne koblingen åpnes vinduet **Beskyttelsesomfang for File Anti-Virus**, som inneholder en liste over objekter som skannes av File Anti-Virus. Du kan legge til objekter i listen eller slette objektene du legger til. Hvis du vil fjerne et objekt fra skanningen, trenger du ikke å slette objektet fra listen. Du trenger bare å fjerne avmerkingen i boksen ved siden av objektnavnet.
Heuristisk analyse	En teknikk for å oppdage trusler som ikke kan identifiseres ved å bruke den gjeldende versjonen av programdatabasene til Kaspersky. Den lar deg finne filer som kan inneholde ukjent skadelig programvare eller en ny modifisering av kjent skadelig programvare. Når du skanner filer etter skadelig kode, utfører den heuristiske analysen instruksjoner i de kjørbare filene. Antall instruksjoner som utføres av den heuristiske analysen, avhenger av nivået som er angitt for den heuristiske analysen. Det heuristiske analysenivået angir balansen mellom grundighetsnivået på søket etter nye trusler, belastningen på operativsystemets ressurser og tiden som kreves for den heuristiske analysen.
Skann kun nye og endrede filer	Skanner bare nye filer og filene som er endret siden sist de ble skannet sist. På denne måten kan du spare tid på skanningen. Denne skannemodusen gjelder både for enkle og sammensatte filer.
Skann arkiver	Skann ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE og andre arkiver. Programmet skanner arkiver ikke bare etter utvidelsene, men også etter formatene deres.
Skann distribusjonspakker	Avmerkingsboksen aktiverer/deaktiverer skanning av distribusjonspakker fra tredjeparter.
Skann filer med Microsoft Office-format	Skanner Microsoft Office-filer (DOC, DOCX, XLS, PPT og andre Microsoft-filtyper). Microsoft Office-filer inkluderer også OLE-objekter.
Ikke pakk ut store sammensatte filer **Maksimal filstørrelse**	Hvis avmerkingsboksen er valgt, skanner ikke programmet sammensatte filer som er større enn den angitte verdien. Hvis alternativet er deaktivert, skanner programmet sammensatte filer av enhver størrelse. Programmet skanner store filer som er hentet fra arkiver, uavhengig av om avmerkingsboksen er aktivert eller ikke.
Pakk ut sammensatte filer i bakgrunnen **Minimal filstørrelse**	Hvis denne avmerkingsboksen er aktivert, gir programmet tilgang til sammensatte filer som er større enn den angitte verdien, før disse filene blir skannet. I dette tilfellet pakker Kaspersky-programmet ut og skanner sammensatte filer i bakgrunnen. Programmet gir tilgang til sammensatte filer som er mindre enn denne verdien, men bare etter at disse filene er pakket ut og skannet. Hvis denne avmerkingsboksen ikke er aktivert, gir programmet tilgang til sammensatte filer bare etter at filene er pakket ut og skannet, uavhengig av størrelsen.

Skannemodus	**Smartmodus**. I denne modusen skanner File Anti-Virus et objekt basert på en analyse av handlingene som er utført med det objektet. Hvis du for eksempel arbeider på et Microsoft Office-dokument, skanner Kaspersky-programmet filen første gang den åpnes og siste gang den lukkes. Mellomliggende operasjoner som overskriver filen, fører ikke til at filen skannes. **Ved tilgang og endring**. I denne modusen skanner File Anti-Virus objekter ved forsøk på å åpne/endre dem. **Ved tilgang**. I denne modusen skanner File Anti-Virus objekter kun ved forsøk på å åpne dem. **Ved kjøring**. I denne modusen skanner File Anti-Virus bare objekter ved forsøk på å kjøre dem.
iSwift-teknologi	Denne teknologien er en videreutvikling av iChecker-teknologi for datamaskiner som benytter NTFS-filsystemet. Det finnes begrensninger med iSwift-teknologien: Den er knyttet til en bestemt fils plassering i filsystemet og kan kun brukes for objekter i NTFS-filsystemet. Når du oppgraderer Kaspersky-programmet til en ny versjon, er iSwift-teknologien aktivert for alle typer skanning, selv om den tidligere var deaktivert.
iChecker-teknologi	Denne teknologien gjør det mulig å øke skannehastigheten ved å utelate bestemte filer fra skanning. En fil utelates fra skanning med en spesiell algoritme som tar hensyn til utgivelsesdatoen for Kaspersky-programmets databaser, datoen filen sist ble skannet og eventuelle endringer gjort for skanneinnstillingene. Det finnes begrensninger med iChecker-teknologien: Den fungerer ikke med store filer og gjelder kun for filer med en struktur som programmet gjenkjenner (for eksempel EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP og RAR).
Unntak	Objekter ekskludert fra skanninger. Hvis du vil angi unntak, klikker du på **Behandle unntak** i vinduet **Unntak**.
Sett File Anti-Virus på pause	Dette avbryter automatisk driften av File Anti-Virus midlertidig på det angitte tidspunktet eller når du arbeider med de angitte programmene. Du kan konfigurere dette ved å klikke på koblingen **Sett File Anti-Virus på pause**.

Innstillinger for AMSI-beskyttelse

Innstillinger	Beskrivelse
Skann arkiver	Skann ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE og andre arkiver. Programmet skanner arkiver ikke bare etter utvidelsene, men også etter formatene deres.
Skann distribusjonspakker	Avmerkingsboksen aktiverer/deaktiverer skanning av distribusjonspakker fra tredjeparter.
Skann filer med Microsoft Office-format	Skanner Microsoft Office-filer (DOC, DOCX, XLS, PPT og andre Microsoft-filtyper). Microsoft Office-filer inkluderer også OLE-objekter.
Ikke pakk ut store sammensatte filer **Maksimal filstørrelse**	Hvis avmerkingsboksen er valgt, skanner ikke programmet sammensatte filer som er større enn den angitte verdien. Hvis alternativet er deaktivert, skanner programmet sammensatte filer av enhver størrelse. Programmet skanner store filer som er hentet fra arkiver, uavhengig av om avmerkingsboksen er aktivert eller ikke.

Vinduet Legg til / rediger personlige data

Typer personlige data

Når du klikker på koblinger i feltet **Feltnavn**, vises den tilsvarende typen med personlige data.

Feltnavn

Beskrivelse som vises i listen over oppføringer med personlige data (for eksempel *Hjemmetlf*, *Kontortlf*, *postnummer*).

Du kan kopiere beskrivelsen av personlige data automatisk ved å klikke på den tilsvarende koblingen med typen personlige data.

Verdi

Personlige data som skal kunne sendes eller ikke.

Rapport om overføring av personlige data

Navnet på brukerkontoen som det rapporteres handlinger om i dette vinduet, vises øverst i vinduet.

Kontroll er aktivert/deaktivert  /

Denne bryteren brukes til å aktivere/deaktivere overvåking av brukerhandlinger av Foreldrekontroll.

Knappen kan ha følgende utseende, avhengig av om Foreldrekontroll overvåker brukerens handlinger eller ikke:

 – Foreldrekontroll overvåker brukerens handlinger.

 – Foreldrekontroll overvåker ikke brukerens handlinger.

Overvåkingen utføres i henhold til innstillingene for den aktuelle brukeren i Foreldrekontroll.

I dette vinduet kan du vise informasjon om den valgte brukerens bruk av nøkkelord og forsøk på å overføre personlige data.

I dag

Klikk på denne knappen for å åpne rapporten om brukerens aktiviteter i dag.

Knappene

Klikk på disse knappene for å åpne rapporter om foregående og etterfølgende perioder.

Dag/uke/måned

Perioden som den opprettede rapporten gjelder for. Du kan opprette en rapport for følgende perioder: dag, uke og måned.

Knappen

Klikk på denne knappen for å åpne innstillingsvinduet i Foreldrekontroll med delen **Innholdskontroll** åpen. I denne delen kan du definere begrensninger for sending av personlige data.

Liste over blokkerte personlige data

Inneholder listen over personlige data fra meldinger som er sendt og mottatt av den valgte brukeren i løpet av den angitte perioden.

Data

Denne kolonnen inneholder personlige data fra sendte og mottatte meldinger.

Når det gjelder blokkering av personlige data, er typen informasjon som skal blokkeres, angitt.

Ressurs

Denne kolonnen viser et nettsted som brukeren har benyttet for å prøve å sende eller motta en melding som inneholder personlige data du vil blokkere overføring av.

Status

Hvis sending av meldingen er blokkert av Foreldrekontroll, vil du også se statusen *Blokkert*.

Dato

Denne kolonnen viser datoen for mottak eller sending av meldingen som inneholder personlige data som er blokkert fra å overføres.

Velge en brukerprofil

Datainnsamling

Klikk på denne knappen for å bruke profilen med standardinnstillinger på kontoen til den valgte brukeren. Denne profilen henter kun inn statistikk om handlingene til valgt bruker. Begrensninger av program- og Internett-bruk er ikke angitt.

Egendefinerte begrensninger

Manuelt konfigurerte innstillinger blir brukt for den valgte brukerens konto.

Barn (4+)

Klikk på denne knappen for å bruke profilen som er beregnet på barn fra 4 til 12 år, på kontoen til den valgte brukeren. Denne profilen inneholder følgende regler for bruk av Internett og programmer:

- Internett-bruk tillatt
- Surfing på nettet er kun tillatt for nettsteder som er oppført i kategoriene «Internettkommunikasjon» og «Dataspill».
- Nedlasting av alle typer filer er blokkert.
- Kontroll av datamaskinbruk er aktivert, men ingen begrensninger er definert.
- Overvåking av programbruk er aktivert, men ingen begrensninger er i bruk.
- Overvåking av spillbruk er aktivert; begrensninger angis i henhold til klassifiseringssystemet.

Tenåring (12+)

Klikk på denne knappen for å bruke profilen som er beregnet på barn over 12 år, på kontoen til den valgte brukeren. Denne profilen inneholder følgende regler for bruk av Internett og programmer:

- Internett-bruk tillatt
- Surfing på nettet er kun tillatt for nettsteder som er oppført i kategoriene «Internett-kommunikasjon», «Shopping, banker, betalingssystemer» og «Dataspill».
- Kontroll av datamaskinbruk er aktivert, men ingen begrensninger er definert.
- Overvåking av programbruk er aktivert, men ingen begrensninger er i bruk.
- Overvåking av spillbruk er aktivert; begrensninger angis i henhold til klassifiseringssystemet.

Standardinnstillinger

Klikk på denne knappen for å bruke profilen med standardinnstillinger på kontoen til den valgte brukeren. Denne profilen inneholder følgende regler for bruk av Internett og programmer:

- Internett-bruk tillatt
- Surfing på nettet er kun tillatt for nettsteder som er oppført i kategoriene «Internett-kommunikasjon», «Shopping, banker, betalingssystemer» og «Dataspill».
- Sikkert søk er aktivert.
- Kontroll av datamaskinbruk er aktivert, men ingen begrensninger er definert.
- Overvåking av programbruk er aktivert, men ingen begrensninger er i bruk.
- Overvåking av spilloppstart er aktivert; ingen oppstartsbegrensninger er angitt.
- Overvåking av krypterte SSL-tilkoblinger i nettlesere er aktivert.

Importer

Klikk på denne koblingen for å åpne et vindu der du kan velge filen som inneholder innstillinger for Foreldrekontroll. Når du har valgt filen, brukes innstillingene på kontoen til den valgte brukeren.

Eksporter

Klikk på denne koblingen for å åpne et vindu der du kan lagre de gjeldende innstillingene for Foreldrekontroll i en fil.

Vinduet Legg til / rediger nettadresse

Nettadressemaske

Nettadressen eller adressemasken til nettstedet som du vil blokkere eller tillate tilgang til.

Handling

Brukes til å blokkere eller tillate brukerens tilgang til nettsteder.

Du kan velge ett av følgende alternativer:

- **Tillat**. Hvis du velger dette alternativet, vil Foreldrekontroll tillate tilgang til nettstedet selv om det tilhører en blokkert kategori eller om blokkering av alle nettsteder er aktivert.
- **Blokker**. Hvis du velger dette alternativet, vil Foreldrekontroll blokkere tilgang til nettstedet selv om det tilhører en tillatt kategori.

Type

Du kan angi omfanget som innstillingene for tilgang til nettstedet skal gjelde.

Du kan velge ett av følgende alternativer:

- **Nettstedmaske**. Hvis du velger dette alternativer, vil Foreldrekontroll tillatte eller blokkere brukerens tilgang til alle nettstedene på det angitte nettstedet.

  Hvis for eksempel feltet **Nettadressemaske** inneholder adressen eksempel.no, vil Foreldrekontroll tillate eller blokkere tilgang til alle nettsider på eksempel.no, inkludert nyheter.eksempel.no, marked.eksempel.no og post.eksempel.no.

- **Spesifisert nettadresse**. Hvis du velger dette alternativet, vil Foreldrekontroll tillate eller blokkere brukerens tilgang kun til den angitte siden på nettstedet som er angitt i feltet **Nettadressemaske**.

  Hvis du for eksempel spesifiserer URL-adressen mail.example.com/login i feltet **Nettadressemaske**, vil Foreldrekontroll tillate eller blokkere tilgang kun til den angitte påloggingssiden som brukes til å logge på denne e-postkontoen. Denne regelen vil ikke gjelde for andre sider på nettstedet.

Bruk mal

Gjør det mulig å bruke unntaket på en av de eksisterende malene, med det spesifiserte innstillingssettet.

Du kan velge ett av følgende alternativer:

- **Hele nettstedet** – Når dette alternativet er valgt, vil Foreldrekontroll tillate eller blokkere tilgang til domenet som er spesifisert i feltet **Nettadressemaske**. Hvis for eksempel feltet **Nettadressemaske** inneholder adressen eksempel.no, vil Foreldrekontroll tillate eller blokkere tilgang til alle websider på domenet eksempel.no, inkludert nyheter.eksempel.no, marked.eksempel.no og post.eksempel.no.

- **Spesifisert nettside** – når dette alternativet er valgt, vil Foreldrekontroll tillate eller blokkere tilgang til siden som er spesifisert i feltet **Nettadressemaske**, og til alle nettadresser som inneholder denne siden. Hvis feltet **Nettadressemaske** for eksempel inneholder adressen eksempel.no/hl, vil Foreldrekontroll tillate eller blokkere tilgang til både denne siden og nettadresser den ligger på, som for eksempel.no/hl/eksempel1.html.

- **Spesifisert nettadresse** – Når dette alternativet er valgt, vil Foreldrekontroll tillate eller blokkere tilgang til den bestemte nettadressen angitt i feltet **Nettadressemaske**. Hvis du for eksempel spesifiserer URL-adressen mail.example.com/login i feltet **Nettadressemaske**, vil Foreldrekontroll tillate eller blokkere tilgang kun til den angitte påloggingssiden som brukes til å logge på denne e-postkontoen. Denne regelen vil ikke gjelde for andre sider på nettstedet.

Unntak fra Foreldrekontroll

I dette vinduet kan du lage en liste med unntak fra de konfigurerte innstillingene for Foreldrekontroll. Tilgangsinnstillinger som påvirker nettsteder lagt til i unntakslisten gjelder både ved blokkering av nettsteder etter kategorier (knappen **Blokker tilgang til nettsteder fra valgte kategorier**) og ved blokkering av alle nettsteder (knappen **Blokker tilgang til alle nettsteder**).

Du kan for eksempel tillate tilgang til nettsteder i kategorien Internettkommunikasjon, men legge til www.example.com i listen over unntak for å blokkere tilgang til dette nettstedet. I dette tilfellet vil Foreldrekontroll tillate tilgang til alle sosiale nettverk, unntatt det sosiale nettverket eksempel.com. Du kan også blokkere alle nettsteder og legge til et nettsted for e-post, som du kan tillate tilgang til ved å legge det til i listen over unntak. I dette tilfellet vil Foreldrekontroll kun gi brukeren tilgang til e-postområdet.

Liste over unntak

Listen inneholder nettadresser som er blokkert eller tillatt, uavhengig av innstillingene i Foreldrekontroll.

Du kan bruke hurtigmenyen til nettadressen på listen når du vil endre nettadressen, fjerne den fra listen eller tillate eller blokkere tilgang til nettstedet.

Nettadressemaske

Nettadressen eller nettadressemasken til nettstedet som er blokkert eller tillatt.

Type

Kolonnen viser omfanget som nettstedets tilgangsinnstillinger skal brukes på.

Hvis alternativet *Nettstedmaske* vises i kolonnen, er tilgang til alle sidene på nettstedet tillatt eller blokkert.

Hvis alternativet *Spesifisert nettadresse* vises i kolonnen, er kun tilgang til den angitte nettsiden på nettstedet tillatt eller blokkert.

Handling

Denne kolonnen viser om tilgang til nettstedet er tillatt eller blokkert.

Hvis alternativet *Tillatt* vises i kolonnen, tillater Foreldrekontroll tilgang til nettstedet.

Hvis alternativet *Blokkert* vises i kolonnen, blokkerer Foreldrekontroll tilgang til nettstedet.

Rediger

Klikk på denne knappen for å åpne vinduet **Rediger**, der du kan redigere nettadressemasken eller nettadressen til nettstedet som er valgt i listen over unntak og i innstillingene for tilgang til nettstedet.

Knappen er tilgjengelig når en nettadressemaske er valgt i unntakslisten.

Slett

Klikk på denne knappen for å fjerne den valgte nettadressemasken fra listen over unntak.

Knappen er tilgjengelig når en nettadressemaske er valgt i unntakslisten.

Legg til

Klikk på denne knappen for å åpne vinduet for å legge til en adressemaske for et nettsted, der du kan legge til en nettadresse eller en adressemaske i listen over unntak.

Vinduet Begrensning av programbruk

I dette vinduet kan du definere begrensinger for bruk av et valgt program.

I delen **Ukedager** kan du begrense bruk av programmet på ukedager.

Tillat tilgang i maksimalt <N> timer per dag

Dette alternativer aktiverer/deaktiverer tidsbegrensningen for bruk av programmet på ukedager.

Hvis alternativet er aktivert, begrenser Foreldrekontroll den valgte brukerens totale bruk av programmet. Tidsbegrensningen for programmet velges (i timer) fra rullegardinlisten ved siden av avkryssingsboksen.

Hvis alternativet er deaktivert, begrenser ikke Foreldrekontroll bruk av programmet på ukedager.

I delen **Helger** kan du begrense bruk av programmet i helgene.

Tillat tilgang i maksimalt <N> timer per dag

Dette alternativer aktiverer/deaktiverer tidsbegrensningen for bruk av programmet i helgene.

Hvis alternativet er aktivert, begrenser Foreldrekontroll den valgte brukerens totale bruk av programmet. Tidsbegrensningen for programmet velges (i timer) fra rullegardinlisten ved siden av avkryssingsboksen.

Hvis alternativet er deaktivert, begrenser ikke Foreldrekontroll bruk av programmet i helgene.

I delen **Pauser** kan du definere periodisk blokkering av programtilgang i løpet av dagen.

Ta en pause hver <N> time i <N> minutter

Alternativet aktiverer/deaktiverer periodisk blokkering av programmet i angitte tidsperioder for å passe på at brukeren tar en pause.

Hvis alternativet er aktivert, vil Foreldrekontroll blokkere programmet i perioden som er angitt i rullegardinlisten **<TT:MM>**. Tilgang er blokkert for perioden som er valgt fra rullegardinlisten **<N> minutter**.

Delen **Nøyaktig brukstid** viser en tabell over tider for programbruk. Du kan bruke denne tabellen til å definere en timebasert tidsplan for bruk av programmet i løpet av uken.

Timeplan for programbruk

Du kan bruke denne tabellen til å angi ukedagene og tidspunktene som brukeren kan bruke programmet på. Tabellradene representerer ukedagene, og tabellkolonnene representerer én-timers intervaller innenfor tidsskalaen. Avhengig av de regionale innstillingene til operativsystemet vil tidsskalaen være 24-timers eller 12-timers. Tabellcellenes farger angir aktive begrensninger: Rød betyr at programbruk er blokkert, og grå betyr at programmet kan brukes. Tabellcellen endrer farge når du klikker på den. Når du ruller musepekeren over en celle, vises tidsintervallet for denne cellen under tabellen.

Vinduet Liste over personlige data

Liste over personlige data

Denne listen inneholder brukerens personlige data, og sending av slike data skal kontrolleres.

Feltnavn

Denne kolonnen viser typen personlige data (for eksempel *Bankkortnummer* eller *Hjemmetelefonnummer*).

Verdi

Denne kolonnen inneholder personlige data (for eksempel bankkortnumre, telefonnumre osv.) som bør overvåkes i meldinger.

Rediger

Når du klikker på denne knappen, åpnes et vindu der du kan redigere en oppføring med personlige data.

Slett

Hvis du klikker på denne knappen, fjerner du den valgte oppføringen fra listen.

Legg til

Når du klikker på denne knappen, åpnes et vindu der du kan legge til en ny oppføring i listen over personlige data.

Rapport for blokkerte nettsteder og nedlastinger

I dag

Klikk på denne knappen for å åpne rapporten om brukerens aktiviteter i dag.

Knappene

Klikk på disse knappene for å åpne rapporter om foregående og etterfølgende perioder.

Dag/uke/måned

Perioden som den opprettede rapporten gjelder for. Du kan opprette en rapport for følgende perioder: dag, uke og måned.

Knappen

Klikk på denne knappen for å åpne innstillingsvinduet i Foreldrekontroll med delen **Internett** åpen. I denne delen kan du definere begrensninger for Internett-bruk, tilgang til nettsider og nedlasting av filer for den valgte brukeren.

Blokkerte nettsteder og nedlastinger

Denne listen inneholder nettsteder som er blokkert av Foreldrekontroll og filer som er blokkert for nedlasting.

Listen inneholder følgende data:

- Navnet på det blokkerte nettstedet eller den blokkerte filen.
- Årsaken til at brukerens tilgangsforsøk ble blokkert (for eksempel *nettsted fra blokkert kategori*)
- Datoen da nettstedet ble åpnet eller filen ble nedlastet.

Rapport for programbruk

Navnet på brukerkontoen som det rapporteres handlinger om i dette vinduet, vises øverst i vinduet.

Kontroll er aktivert/deaktivert  / 

Denne bryteren brukes til å aktivere/deaktivere overvåking av brukerhandlinger av Foreldrekontroll.

Knappen kan ha følgende utseende, avhengig av om Foreldrekontroll overvåker brukerens handlinger eller ikke:

 – Foreldrekontroll overvåker brukerens handlinger.

 – Foreldrekontroll overvåker ikke brukerens handlinger.

Overvåkingen utføres i henhold til innstillingene for den aktuelle brukeren i Foreldrekontroll.

I vinduet **Rapport for programbruk** kan du vise informasjon om oppstart av programmer for en valgt konto i løpet av et spesifisert tidsintervall.

I dag

Klikk på denne knappen for å åpne rapporten om brukerens aktiviteter i dag.

Knappene

Klikk på disse knappene for å åpne rapporter om foregående og etterfølgende perioder.

Dag/uke/måned

Perioden som den opprettede rapporten gjelder for. Du kan opprette en rapport for følgende perioder: dag, uke og måned.

Knappen

Klikk på denne knappen for å åpne innstillingsvinduet i Foreldrekontroll med delen **Programmer** åpen. I dette vinduet kan du definere begrensinger for oppstart og bruk av programmer.

Programmer som brukes ofte

Inneholder en liste over programmer som er oftest brukt av brukeren i løpet av den angitte perioden. Listen angir også brukstiden for hvert enkelt program.

Blokkerte programmer

Inneholder en liste over programmer som Foreldrekontroll har blokkert oppstart av. Programmene vises i kronologisk rekkefølge, med de som er startet sist, øverst på listen.

Klikk på koblingen **<N> til** for å vise andre programmer som oppstart er blokkert for.

Alle brukte programmer

Inneholder en liste over alle programmer som brukeren har startet i løpet av den angitte perioden. Listen angir også brukstiden for hvert enkelt program.

Programmer grupperes i kategorier (for eksempel Spill eller Direktemeldingsprogrammer).

Hvis du klikker på ⌄-knappen, åpnes listen over programmer i den aktuelle kategorien.

Hvis du klikker på ›-knappen, åpnes listen over programmer i den aktuelle kategorien til én linje.

Blokker spill etter kategorier

I dette vinduet kan du aktivere eller deaktivere blokkering av spill basert på deres innhold. Klassifisering av spillinnhold (to avmerkingsbokser) er basert på PEGI-eller ESRB-rangeringer. Typen spillklassifisering som skal brukes, velges automatisk avhengig av hvor du befinner deg. Om nødvendig kan du velge typen spillklassifisering manuelt i innstillingene for komponenten Foreldrekontroll.

Hvis det er merket av i boksen ved siden av en kategori, vil Foreldrekontroll blokkere spill i denne kategorien.

Hvis det ikke er merket av i boksen ved siden av en kategori, vil Foreldrekontroll tillate start av spill i denne kategorien.

Et spill kan startes hvis alle kategoriene som er relevante for spillinnholdet, er tillatt.

Vinduet Passordomfang

Styre sikkerhetskopiering og gjenoppretting

Denne avmerkingsboksen aktiverer/deaktiverer alternativet som ber brukeren om å angi et passord for å åpne vinduet **Sikkerhetskopiering og gjenoppretting**.

Konfigurer programinnstillinger

Alternativet aktiverer/deaktiverer anmodning om passord når brukeren forsøker å lagre endringer i programinnstillingene.

Avslutt programmet

Alternativet aktiverer/deaktiverer anmodning om passord når brukeren forsøker å avslutte programmet.

Fjerne programmet

Alternativet aktiverer / deaktiverer anmodning om passord når brukeren forsøker å fjerne programmet.

Opprett passord

Klikk på denne knappen hvis du vil bruke passordbeskyttelse til å begrense tilgang til angitte programfunksjoner.

Generell statistikk

Navnet på brukerkontoen som det rapporteres handlinger om i dette vinduet, vises øverst i vinduet.

Kontroll er aktivert/deaktivert  / 

Denne bryteren brukes til å aktivere/deaktivere overvåking av brukerhandlinger av Foreldrekontroll.

Knappen kan ha følgende utseende, avhengig av om Foreldrekontroll overvåker brukerens handlinger eller ikke:

 – Foreldrekontroll overvåker brukerens handlinger.

 – Foreldrekontroll overvåker ikke brukerens handlinger.

Overvåkingen utføres i henhold til innstillingene for den aktuelle brukeren i Foreldrekontroll.

Profil: <profilinnstillinger>

Ved å klikke på denne lenken kan du konfigurere foreldrekontrollinnstillinger som skal brukes for den nåværende kontoen.

I delen **Datamaskin** kan du vise datamaskinbruken til valgt bruker, vise en rapport over datamaskinbruk og konfigurere innstillinger for Foreldrekontroll. Statistikk over datamaskinbruk vises for tidsperioden som er angitt i rapporten om datamaskinbruk. Som standard vises statistikk for de siste 24 timene.

Detaljer

Klikk på denne lenken for å åpne vinduet **Rapport for datamaskinbruk**. I dette vinduet kan du vise informasjon om den valgte brukerens datamaskinbruk.

Innstillinger

Klikk på denne lenken for å åpne vinduet. I dette vinduet kan du spesifisere tidsperioden der den valgte brukeren kan bruke datamaskinen.

I delen **Programmer** kan du vise detaljer om programmer som den valgte brukeren nylig har kjørt. Statistikk om programbruk vises for tidsperioden som er angitt i rapporten om programbruk. Som standard vises statistikk for de siste 24 timene.

Detaljer

Klikk på denne koblingen for å åpne vinduet **Rapport for programbruk**. Dette vinduet viser informasjon om programmer som har blitt startet av den valgte brukeren, og hvor lenge programmene ble brukt.

Innstillinger

Klikk på denne lenken for å åpne vinduet. I dette vinduet kan du spesifisere hvilke programmer den valgte brukeren kan bruke.

Delen **Internett** inneholder statistikk om besøk på nettsteder og en rapport som viser hvor lenge brukeren besøkte disse nettstedene. Du kan også vise totalt antall blokkerte forsøk på å besøke blokkerte nettsteder.

Statistikk over besøkte webressurser vises for tidsperioden som er angitt i rapporten om Internett-bruk. Som standard vises statistikk for de siste 24 timene.

Detaljer

Klikk på denne koblingen for å åpne vinduet **Rapport for Internett-bruk**. I dette vinduet kan du vise informasjon om webressurser som den valgte brukeren har besøkt.

Innstillinger

Klikk på denne lenken for å åpne vinduet. I dette vinduet kan du spesifisere tidsperioden der den valgte brukeren tillates å bruke Internett.

Delen **Innholdskontroll** viser informasjon om antall blokkerte forsøk på å overføre personlige data.

Statistikken vises for perioden som er angitt i innholdskontrollrapporten. Som standard vises statistikk for en uke.

Detaljer

Klikk på denne lenken for å åpne vinduet. I dette vinduet kan du motta informasjon om hvilke personlige data den valgte brukeren forsøkte å sende i løpet av kommunikasjonen på sosiale nettverk.

Innstillinger

Klikk på denne lenken for å åpne vinduet. I dette vinduet kan du spesifisere de personlige dataene du ønsker å overvåke i samtalene til den valgte brukeren.

Rapport for Internett-bruk

Navnet på brukerkontoen som det rapporteres handlinger om i dette vinduet, vises øverst i vinduet.

Kontroll er aktivert/deaktivert /

Denne bryteren brukes til å aktivere/deaktivere overvåking av brukerhandlinger av Foreldrekontroll.

Knappen kan ha følgende utseende, avhengig av om Foreldrekontroll overvåker brukerens handlinger eller ikke:

– Foreldrekontroll overvåker brukerens handlinger.

– Foreldrekontroll overvåker ikke brukerens handlinger.

Overvåkingen utføres i henhold til innstillingene for den aktuelle brukeren i Foreldrekontroll.

I vinduet **Rapport for Internett-bruk** kan du vise informasjon om nettsteder som den angitte brukeren besøkte i løpet av den angitte perioden.

I dag

Klikk på denne knappen for å åpne rapporten om brukerens aktiviteter i dag.

Knappene

Klikk på disse knappene for å åpne rapporter om foregående og etterfølgende perioder.

Dag/uke/måned

Perioden som den opprettede rapporten gjelder for. Du kan opprette en rapport for følgende perioder: dag, uke og måned.

Knappen

Klikk på denne knappen for å åpne innstillingsvinduet i Foreldrekontroll med delen **Internett** åpen. I denne delen kan du definere begrensninger for Internett-bruk, tilgang til nettsider og nedlasting av filer for den valgte brukeren.

Favorittnettsteder

Denne rapporten viser en liste med nettsteder brukeren besøkte ofte i løpet av rapporteringsperioden, og antall besøk.

Brukt

Den totale tiden som er brukt på Internett, for valgt bruker og valgt periode.

Nettressurser blokkert

Liste over nettsteder som er blokkert av Foreldrekontroll, og liste over filer som er blokkert for nedlasting.

Vis alle

Klikk på denne koblingen for å åpne et vindu med informasjon om antallet blokkerte filnedlastinger og besøk på nettsteder.

Nettstedkategorier

Det inneholder en liste over nettstedkategorier. For hver nettstedkategori vises antallet besøk som er blokkert eller tillatt av Foreldrekontroll:

- Antall forsøk på å få tilgang til nettsteder som er blokkert av Foreldrekontroll, er uthevet i rødt.
- Antall forsøk på å få tilgang til nettsteder som er tillatt av Foreldrekontroll, er uthevet i grått.

Rapport for datamaskinbruk

Navnet på brukerkontoen som det rapporteres handlinger om i dette vinduet, vises øverst i vinduet.

Kontroll er aktivert/deaktivert /

Denne bryteren brukes til å aktivere/deaktivere overvåking av brukerhandlinger av Foreldrekontroll.

Knappen kan ha følgende utseende, avhengig av om Foreldrekontroll overvåker brukerens handlinger eller ikke:

– Foreldrekontroll overvåker brukerens handlinger.

– Foreldrekontroll overvåker ikke brukerens handlinger.

Overvåkingen utføres i henhold til innstillingene for den aktuelle brukeren i Foreldrekontroll.

I vinduet **Rapport for datamaskinbruk** kan du vise informasjon om datamaskinbruken for en valgt konto i løpet av et angitt tidsintervall.

I dag

Klikk på denne knappen for å åpne rapporten om brukerens aktiviteter i dag.

Knappene ‹ ›

Klikk på disse knappene for å åpne rapporter om foregående og etterfølgende perioder.

Dag/uke/måned

Perioden som den opprettede rapporten gjelder for. Du kan opprette en rapport for følgende perioder: dag, uke og måned.

Knappen

Klikk på denne knappen for å åpne innstillingsvinduet i Foreldrekontroll med delen **Datamaskin** åpen. I denne delen kan du angi tidsbegrensninger for datamaskinbruk.

Rapport for datamaskinbruk

Inneholder informasjon om perioder og varighet for datamaskinbruk i den angitte perioden.

Perioder da datamaskinen ble brukt av valgt konto, er uthevet i rosa.

Gjeldende tidsperiode (dag, uke eller måned) er uthevet i grønt.

Gjeldende klokkeslett for dagen (hvis perioden *Dag Uke* er valgt) vises med en rød strek.

Vinduet Styre programmer

Start / Begrensninger

Hvis du vil endre hvordan programmer vises i listen, klikker du på følgende koblinger:

- Når du klikker på koblingen **Start**, sorteres programmene i listen i to grupper: **Blokkert** og **Tillatt**.
- Klikk på koblingen **Begrensninger** for å sortere programmene i listen etter klareringsgrupper. Klarerte programmer oppføres for eksempel i gruppen **Klarert**.

Rydd opp

Klikk på denne koblingen hvis du vil at Kaspersky skal fjerne programmer som ikke finnes lenger, fra listen.

Vis

Fra rullegardinlisten kan du velge visningsmodus for programmer og prosesser.

- **Utvid alle**. Hvis du velger dette elementet, viser listen alle programmene som er installert på datamaskinen.
- **Skjul alle**. Hvis du velger dette elementet, viser listen klareringsgrupper.

Fra rullegardinlisten kan du velge visningsmodus for programmer og prosesser:

- **Vis som liste**. Hvis du velger dette alternativet, vil programmer og prosesser vises som en liste.
- **Trevisning**. Hvis du velger dette alternativet, vil programmene og prosessene vises hierarkisk, basert på rekkefølgen prosessene ble startet i.

I denne rullegardinlisten kan du også deaktivere visning av systemprogrammer, Kaspersky-programmer og programmer utenfor nettverket:

- **Skjul systemprogrammer**. Hvis du velger dette alternativet, vil den generelle listen over programmer og prosesser ikke inneholde programmer som er nødvendige for at operativsystemet skal fungere på riktig måte. Systemprogrammer er skjult som standard.
- **Skjul <PRODUCT>**. Hvis du velger dette alternativet, vil den generelle listen over programmer og prosesser ikke vise Kaspersky-programmer. Kaspersky-programmer er skjult som standard.
- **Vis kun nettverksprogrammer**. Hvis du velger dette alternativet, vil den generelle listen med programmer og prosesser vise kun nettverksprogrammer. Nettverksprogrammer er programmer beregnet for å organisere samarbeid mellom flere brukere på forskjellige datamaskiner.

Programlisten

Denne listen inneholder programmer som er installert på datamaskinen din. Du kan vise informasjon om status, digital signatur, klareringsgruppe, popularitet blant KSN-brukere og tidspunktet da det sist ble startet for hvert program på listen.

Dobbeltklikk på raden til et program eller en prosess for å åpne vinduet **Programregler**. I dette vinduet kan du konfigurere regler for å kontrollere programmets handlinger.

Høyreklikk på raden til programmet for å åpne hurtigmenyen. Fra hurtigmenyen kan du utføre følgende handlinger:

- Åpne vinduet **Programregler**, der du kan konfigurere tillatelser for programaktiviteter.
- Tillat eller blokker oppstart av program.
- Flytte programmet til en annen klareringsgruppe.
- Bruke standardinnstillinger for rettigheter i et program (tilbakestill programinnstillinger).
- Fjerne programmet fra listen.
- Åpne mappen som inneholder den kjørbare filen til programmet.

Programmer i listen inkluderes i grupper og undergrupper. Høyreklikk på raden til gruppen for å åpne hurtigmenyen. Fra hurtigmenyen kan du utføre følgende handlinger:

- Åpne vinduet **Grupperegler**, der du kan sette opp standardtillatelser for handlingene til programmer i denne gruppen.
- Opprett en undergruppe i gruppen. Som standard vil reglene som er spesifisert for gruppen en undergruppe tilhører brukes for denne undergruppen.
- Legg til et program i gruppen. Som standard vil reglene som er spesifisert for gruppen et program tilhører brukes for dette programmet.
- Bruk «Standardinnstillingene for rettigheter i et program» for gruppen og alle undergrupper og programmer i denne gruppen (tilbakestill gruppeinnstillinger).
- Bruk «Standardinnstillingene for rettigheter i et program» for alle undergrupper og programmer i gruppen, men ikke endre gruppens innstillinger (tilbakestill undergrupper og programinnstillinger).
- Slett undergrupper og programmer fra gruppen.

Program

Denne kolonnen viser programmets navn.

Begrensninger

Denne kolonnen viser klareringsgruppen som programmet tilhører. Klareringsgrupper definerer regler for bruk av programmet på datamaskinen: nekte eller tillate oppstart, programmets tilgang til filer og systemregisteret og restriksjoner for programmets nettverksaktivitet.

Popularitet

Denne kolonnen viser programmets popularitet blant deltakerne i Kaspersky Security Network (KSN). Popularitetsnivået avhenger av antallet KSN-deltakere som bruker programmet.

Nettverk

Fra denne kolonnen kan du velge handlingen som skal utføres av programmet når programmet prøver å få tilgang til nettverket.

I tabellen nedenfor finner du en liste over handlingene som skal utføres av Kaspersky når et program eller en programgruppe prøver å få tilgang til nettverket.

Beskrivelse av handlingene til Kaspersky

Handling	Beskrivelse
Arv	Programmet eller gruppen arver responsen fra den overordnede gruppen.
Tillat	Kaspersky tillater at programmene i den valgte gruppen får tilgang til nettverket.
Nekt	Kaspersky blokkerer tilgang til nettverket for programmene i den valgte gruppen.
Spør brukeren	Hvis alternativet **Utfør anbefalte handlinger automatisk** er aktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**, velger Kaspersky handlingen som skal utføres på denne ressursen automatisk basert på regler opprettet av Kasperskys eksperter. Du kan sjekke fotnoten for å lese nøyaktig hvilken handling som blir valgt. Hvis dette alternativet er deaktivert, vil programmet brukeren hvorvidt dette programmet skal tillates å få tilgang til nettverket.
Logg hendelser	Kaspersky registrerer ikke bare den angitte responsen i en rapport, men også informasjon om programmets forsøk på å få tilgang til nettverket.

Start

Bruk bryteren i denne kolonnen til å tillate eller blokkere start av et valgt program. Som standard er start av et program tillatt eller blokkert avhengig av restriksjonene som gjelder for gruppen programmet tilhører.

Beskytte datamaskinen din

Kaspersky-programmet gir omfattende beskyttelse mot virus, nettverksangrep, phishing, brudd på sikkerheten til personlige data og andre typer nettsikkerhetstrusler. Ulike funksjoner og beskyttelseskomponenter er tilgjengelige som en del av Kaspersky-programmet for å gi fullstendig beskyttelse.

Hver enkelt trusseltype behandles av en bestemt komponent. Du kan aktivere og deaktivere beskyttelseskomponenter samt konfigurere komponentenes innstillinger.

Selv om sikkerhetskomponentene gir kontinuerlig datamaskinbeskyttelse, anbefaler vi at du skanner datamaskinen regelmessig etter virus og andre skadelige programmer. Dette er nødvendig for å forhindre eventuell spredning av skadelige programmer som ikke er oppdaget av beskyttelseskomponentene, for eksempel på grunn av at sikkerhetsnivået er satt for lavt, eller av andre årsaker.

Databaser og programmoduler må oppdateres jevnlig for å holde Kaspersky-programmet oppdatert.

Fil-Antivirus

Fil-Antivirus hindrer infeksjon av datamaskinens filsystem. Komponentene starter ved oppstart av operativsystemet, kjører kontinuerlig i datamaskinens minne (RAM), og skanner alle filer som blir åpnet, lagret eller kjørt på datamaskinen og alle tilhørende stasjoner. Kaspersky-programmet fanger opp alle forsøk på å få tilgang til en fil, og skanner filen etter kjente virus og andre skadelige programmer. Ytterligere tilgang til filen er bare tillatt hvis filen ikke er infisert, eller den er desinfisert av programmet. Hvis en fil av en eller annen årsak ikke kan desinfiseres, slettes den. En kopi av filen flyttes da til Karantene. Hvis en infisert fil lagres på plasseringen der en slettet fil med samme navn var lagret tidligere, vil Karantene kun lagre en kopi av den siste filen. En kopi av den gamle filen med samme navn lagres ikke.

Nettverkangrepsblokkering

Nettverkangrepsblokkering lastes inn når du starter operativsystemet, og skanner innkommende nettverkstrafikk etter aktiviteter som har de samme egenskapene som nettverksangrep. Når det oppdages et angrepsforsøk, blokkerer Kaspersky-programmet umiddelbart alle nettverksaktiviteter fra datamaskinen som forsøker å angripe datamaskinen din.

Sikker surfing

Sikker surfing fanger opp og blokkerer kjøring av skript på nettsteder hvis de anses som en trussel. Sikker surfing overvåker også all nettrafikk og blokkerer tilgang til farlige nettsteder.

E-post-Antivirus

E-post-Antivirus skanner innkommende og utgående e-post på datamaskinen. E-posten er kun tilgjengelig for adressaten hvis den ikke inneholder farlige objekter.

Brannmur

Brannmur sørger for sikkerheten din når du bruker lokale nettverk og Internett. Komponenten filtrerer alle nettverksaktiviteter basert på to typer regler: programregler og pakkeregler.

Brannmur er kun tilgjengelig med Kaspersky Standard, Kaspersky Plus og Kaspersky Premium.

Systemvakt

Komponenten Systemvakt ruller tilbake endringene skadelig eller annen programvareaktivitet har gjort i operativsystemet.

Komponenten beskytter mot skadelig programvare, inkludert:

- Utnyttelser
- Skjermlåser
- Krypteringsprogrammer som krypterer data
- Kryptojacking
- Ransomware som krypterer data eller blokkerer tilgang til filer eller systemet, og som krever løsepenger for å gjenopprette eller få tilgang filene

Vi anbefaler ikke å deaktivere denne komponenten.

Anti-Phishing

Kaspersky-programmet beskytter deg mot å besøke phishing-nettsteder. Et phishing-nettsted er et svindelnettsted som ser ut som nettstedet til en bank, et betalingssystem, en plattform for kryptohandel eller et annet legitimt nettsted. Det kan være ganske vanskelig å skille et phishing-nettsted fra et legitimt nettsted bare basert på utseendet. Å besøke et phishing-nettsted kan føre til tyveri av passord, bankkortinformasjon og andre sensitive personopplysninger.

Personvernrengjøring / Rull tilbake endringer

Dette vinduet viser fremdriften under fjerning av spor etter aktivitetene dine i operativsystemet. Rengjøringsprosessen kan ta litt tid. Det kan hende du må starte datamaskinen på nytt for å fjerne enkelte aktivitetsspor.

Hvis du valgte **Rull tilbake endringer** på første trinn, tilbakestiller veiviseren for personvernrengjøring handlinger som ble valgt på forrige trinn.

PC-ressursforbruk

Innstillinger	Beskrivelse
Utfør anbefalte handlinger automatisk	Hvis dette alternativet er deaktivert, er de viktigste komponentene i Kaspersky-programmet i interaktiv modus. Dette betyr at Kaspersky-programmet ber deg om å bestemme hvilken handling du vil utføre på oppdagede objekter og trusler hvis alternativet **Spør brukeren** er valgt i innstillingene for File Antivirus, Sikker surfing, E-post-Antivirus, Systemvakt og Inntrengningsbeskyttelse. Hvis alternativet er valgt, velger Kaspersky-programmet handlingen automatisk basert på regler definert av Kasperskys eksperter.
Slett skadelige verktøy, annonseprogrammer, programmer som automatisk foretar anrop og mistenkelige pakker	Hvis alternativet er valgt, sletter Kaspersky-programmet skadelige verktøy, annonseprogrammer, programmer som automatisk foretar anrop og mistenkelige pakker i automatisk beskyttelsesmodus. Funksjonen er tilgjengelig hvis boksen **Utfør anbefalte handlinger automatisk** er valgt.
Batterisparer	Hvis alternativet er valgt, er energisparingsmodus aktivert. Kaspersky-programmet utsetter planlagte oppgaver. Du kan starte skanning og oppdatere oppgaver manuelt ved behov.
Spillmodus	Hvis alternativet er aktivert, vil ikke Kaspersky-programmet kjøre skanne- eller oppdateringsoppgaver. Det vil heller ikke vise varslinger mens du spiller spill eller kjører programmer i full skjerm.
Ikke forstyrr-modus	Hvis avmerkingsboksen er valgt, viser ikke Kaspersky-programmet hendelsesvarsler under videosamtaler og når du ser på videoer.
Utsett skanneoppgaver når det er høy belastning på prosessoren og disksystemene	Når Kaspersky-programmet kjører planlagte oppgaver, kan dette føre til ekstra arbeidsbelastning på mikroprosessoren og diskenes delsystemer øke, noe som påvirker ytelsen til andre programmer. Når alternativet er valgt, setter Kaspersky-programmet planlagte oppgaver på vent når det oppdager økt belastning for å frigjøre operativsystemressurser for brukerprogrammer.
Skanning etter svake operativsysteminnstillinger	Hvis dette alternativet er aktivert, vil Kaspersky-programmet søke automatisk etter svake innstillinger i operativsystemet.
Start <PRODUCT> ved oppstart av datamaskinen (anbefales)	Når alternativet er aktivert, startes Kaspersky-programmet etter at operativsystemet er lastet inn, og beskytter datamaskinen under hele økten. Når alternativet er deaktivert, startes ikke Kaspersky-programmet etter at operativsystemet er lastet inn, før brukeren starter det manuelt. Databeskyttelse er deaktivert, og brukerdata kan bli utsatt for trusler.
Bruk avansert desinfiseringsteknologi (krever betydelige dataressurser)	Hvis alternativet er aktivert, vises et popup-varsel på skjermen når skadelig aktivitet oppdages i operativsystemet. Varselet fra Kaspersky-programmet tilbyr brukeren å kjøre avansert desinfisering av datamaskinen. Kaspersky-programmet nøytraliserer trusselen etter at brukeren har godkjent dette. Kaspersky-programmet starter datamaskinen på nytt etter å ha kjørt avansert desinfisering. Den avanserte desinfeksjonsteknologien bruker betydelige databehandlingsressurser, noe som kan gjøre andre programmer tregere.

	Det kan hende at enkelte funksjoner i operativsystemet ikke er tilgjengelige mens programmet oppdager en aktiv infeksjon. Tilgjengeligheten til operativsystemet gjenopprettes etter at avansert desinfeksjon er fullført og datamaskinen er startet på nytt.
Søk automatisk etter måter å gjøre PC-en raskere på	Hvis avmerkingsboksen er valgt, utføres det automatiske søk etter måter å øke hastigheten på datamaskinen.
Aktiver Selvforsvar	Når dette alternativet er aktivert, forhindrer Kaspersky endring eller sletting av programfiler på harddisken, minneprosesser og oppføringer i systemregistret.
Tillat administrering av innstillingene for <PRODUCT> via fjernstyringsprogrammer	Hvis dette alternativet er valgt, vil klarerte fjernstyringsprogrammer (f.eks. TeamViewer, LogMeIn Pro og Remotely Anywhere) kunne endre innstillingene for Kaspersky. Ikke klarerte fjernstyringsprogrammer vil ikke kunne endre innstillingene for Kaspersky, selv om dette alternativet er valgt.
Deaktiver ekstern behandling av systemtjenester	Hvis alternativet er valgt, tillater Kaspersky at en ekstern datamaskin å fjernstyrer programtjenester. Når du prøver å fjernstyre programtjenester, vises et varsel ovenfor programikonet på oppgavelinjen i Microsoft Windows (med mindre varslingstjenesten er deaktivert av brukeren).
Aktiver dumpskriving	Hvis alternativet er valgt, skriver Kaspersky til dumpminnet når programmet krasjer. Hvis alternativet er deaktivert, skriver ikke Kaspersky til dumpminnet. Programmet sletter også eksisterende dumpfiler fra datamaskinens harddisk.
Aktiver beskyttelse av dump- og sporingsfiler	Hvis alternativet er aktivert, får både systemadministratoren, den lokale administratoren og brukeren som aktiverte dumpskriving tilgang til dumpfiler. Det er kun systemadministratorer og lokale administratorer som har tilgang til sporingsfiler. Hvis alternativet er deaktivert, kan enhver bruker få tilgang til dumpfiler og sporingsfiler.

Trusler og unntak

Innstillinger	Beskrivelse
Typer oppdagede objekter	Programmet oppdager forskjellige typer objekter, for eksempel virus og ormer, trojanere og annonseprogrammer. Se Kasperskys virusleksikon for mer informasjon. Du kan deaktivere gjenkjenning av følgende typer objekter: • Annen programvare som kriminelle kan bruke til å skade datamaskinen eller dine personlige data. Denne programvaren inkluderer programmer for ekstern administrasjon som systemadministratorer kan bruke til å gå inn i grensesnittet til en ekstern datamaskin for å overvåke og administrere den. • Flerpakkede filer. Filer som er pakket flere ganger, inkludert av forskjellige pakkere. Flerpakking gjør det vanskeligere å skanne objekter.

Behandle unntak	Klikk på denne koblingen for å åpne vinduet **Unntak** med en liste over skanneunntak. Et *skanneunntak* er et sett med betingelser som, når de er oppfylt, fører til at programmet ikke skanner et bestemt objekt for virus og andre trusler.
	Du kan legge til, redigere eller slette unntak fra listen.
	I vinduet der du legger til eller redigerer et unntak, kan du definere bestemte forhold som forhindrer at objekter skannes (programmet vil ikke skanne dem) hvis forholdene er oppfylt:
	• Fil eller mappe som skal unntas fra skanning (du kan også unnta de kjørbare filene til programmer og prosesser). Du kan bruke masker i henhold til følgende regler:
	  • Tegnet `*` (stjerne), som tar plassen til hvilket som helst sett med tegn, unntatt tegnene `\` og `/` (skilletegn for navnene til filer og mapper i banene til filer og mapper). For eksempel vil masken `C:\*\*.txt` inkludere alle baner til filer som har filtypen TXT og er plassert i mapper på C:-stasjonen, men ikke i undermapper.
	  • To påfølgende `*`-tegn tar plassen til hvilket som helst sett med tegn (inkludert et tomt sett) i fil- eller mappenavnet, inkludert tegnene `\` og `/` (skilletegn for navnene til filer og mapper i banene til filer og mapper). For eksempel vil masken `C:\Folder\**\*.txt` inkludere alle banene til filer som har filtypen TXT og er plassert i mappen `Folder`, utenom `Mappen` i seg selv. Masken må inneholde minst ett nestingnivå. Masken `C:\**\*.txt` er ikke en gyldig maske.
	  • Tegnet `?` (spørsmålstegn) tegn, som tar plassen til hvilket som helst tegn, unntatt tegnene `\` og `/` (skilletegn for navnene til filer og mapper i banene til filer og mapper). For eksempel vil masken `C:\Folder\???.txt` inkludere banene til alle filer som ligger i mappen `Folder` og har filtypen TXT og et navn som består av tre tegn.
	• Type objekter som må unntas fra skanninger. Skriv inn navnet til objekttypen i henhold til klassifiseringen av Kasperskys virusleksikon (for eksempel `E-postorm`, `Rotsett` eller `Ekstern administrator`). Du kan bruke masker med tegnet `?` (erstatter ett tegn) og tegnet `*` tegnet (erstatter et hvilket som helst antall tegn). Hvis for eksempel masken `Client*` er angitt, utelukker programmet `Client-IRC-`, `Client-P2P-` og `Client-SMTP-` objekter fra skanninger.

	• Objekters kontrollsum. Ved å sammenligne kontrollsummen til et objekt med kontrollsummen som er angitt i denne innstillingen, kan skanningen ekskludere et objekt som ikke er endret siden forrige skanning. • Beskyttelseskomponenter som unntak gjelder for. I stedet for å slette et unntak fra listen, kan du endre statusen til et unntak til **Inaktiv** (i vinduet der du kan legge til eller redigere et unntak). Unntaket ikke brukt når statusen er Inaktiv.
Angi klarerte programmer	Klikk på denne knappen for å åpne et vindu som viser en liste over klarerte programmer. Kaspersky-programmet overvåker ikke filaktiviteten og nettverksaktiviteten til klarerte programmer (inkludert skadelige klarerte programmer), og overvåker ikke disse programmenes spørringer til systemregistret. Du kan legge til, redigere eller slette klarerte programmer fra listen. Selv om et program er på listen over klarerte programmer, fortsetter Kaspersky-programmet å skanne den kjørbare filen og prosessen til dette programmet for virus og andre trusler. Hvis du ikke vil skanne den kjørbare filen og prosessen til et klarert program, legger du til programmet i listen over unntak. I vinduet **Unntak for program** kan du spesifisere regler som skal brukes av Kaspersky-programmet når du legger til eller redigerer et klarert program, slik at du kan overvåke aktiviteten til det klarerte programmet. I vinduet **Unntak for program** finner du følgende regler: • Ikke skann åpnede filer. • Ikke overvåk programaktivitet. Inntrengningsbeskyttelse overvåker ingen programaktiviteter. • Ikke arve begrensninger fra den overordnede prosessen (til programmet). Hvis begrensninger for overordnede prosesser eller programmer ikke arves, overvåkes programaktivitet i henhold til reglene du har definert eller i henhold til reglene i klareringsgruppen programmet tilhører. • Ikke overvåk underordnet programaktivitet. • Ikke blokker samhandling med grensesnittet til Kaspersky-programmet Programmet tillates å administrere Kaspersky-programmet ved å bruke det grafiske grensesnittet. Du må eventuelt tillate at programmet styrer grensesnittet til Kaspersky-programmet når du bruker et program for tilkobling til eksternt skrivebord eller et program som støtter handlingene til en dataregistreringsenhet. Eksempler på slike enheter omfatter berøringsputer og grafiske nettbrett. • Ikke skann all trafikk (eller kryptert trafikk). Avhengig av det valgte alternativet (**Ikke skann all trafikk** eller **Ikke skann kryptert nettverkstrafikk**), unntar Kaspersky-programmet all nettverkstrafikk i programmet eller trafikk som overføres via SSL fra å bli skannet. Verdien i denne innstillingen påvirker ikke brannmuren: Den skanner programtrafikk i henhold til innstillingene for brannmuren. Unntak påvirker E-post-Antivirus, Sikker surfing og Anti-Spam. Du kan angi IP-adressene eller nettverksportene begrensningen for trafikkontroll må gjelde for.

	Hvis du endrer et programs status til **Inaktiv** i vinduet **Unntak for program**, behandler ikke Kaspersky-programmet som et klarert program. På denne måten kan du midlertidig ekskludere et program fra den klarerte listen, uten å slette det fra listen.
Klarert systemsertifikatlager	Hvis ett av de klarerte systemsertifikatlagrene er valgt, ekskluderer Kaspersky-programmet programmer som er signert med en klarert digital signatur fra skanninger. Kaspersky tilordner slike programmer automatisk til gruppen **Klarert**. Hvis **Ikke bruk** er valgt, skanner Kaspersky programmer uavhengig av om de har en digital signatur eller ikke. Kaspersky-programmet plasserer et program i en klareringsgruppe avhengig av farenivået det aktuelle programmet kan utgjøre for datamaskinen.

Nettverksinnstillinger

Innstillinger	Beskrivelse
Begrens trafikk på kostnadspliktige tilkoblinger	Hvis alternativet er aktivert, begrenser programmet sin egen nettverkstrafikk når Internett-tilkoblingen er begrenset. Kaspersky-programmet identifiserer en høyhastighets Internett-tilkobling som en begrenset tilkobling, og identifiserer en trådløs tilkobling som en ubegrenset tilkobling. Kostnadsbevisst bruk av nettverk fungerer på datamaskiner som kjører Windows 8 eller nyere.
Sett inn skriptet i webtrafikken for å samhandle med nettsider	Hvis du velger dette alternativet, setter Kaspersky-programmet inn et skript i trafikken for å samhandle med websiden. Dette skriptet sikrer driften av komponenter som Safe Money, Privat surfing, Anti-banner og URL-veileder.
Støtter DNS over HTTPS (DoH)	Hvis det er merket av for dette alternativet, behandler programmet DNS-data som overføres over HTTPS, på riktig måte. Vi anbefaler at du ikke fjerner avmerkingen for denne boksen.
Administrer DoH-servere	Koblingen åpner et vindu der du kan legge til en DoH-server manuelt, der DNS-data blir overført i en nettleser. Her kan du lese om DNS via HTTPS (DoH) og hvordan du legger til en DoH-server.
Porter som overvåkes	**Overvåk alle nettverksporter**. I denne modusen for overvåking av porter vil E-post-Antivirus, Anti-Spam og Sikker surfing overvåke alle åpne porter på datamaskinen. **Overvåk kun valgte nettverksporter**. I denne modusen vil E-post-Antivirus, Anti-Spam og Sikker surfing overvåke kun de valgte portene på datamaskinen. Du kan angi nettverksportene som overvåkes i vinduet **Nettverksporter**, som kan åpnes ved å klikke på **Velg**. Du kan også angi for akkurat hvilke programmer overvåking av alle nettverksportene programmene bruker skal være aktivert: • **Overvåk alle porter for programmet fra listen som anbefales av Kaspersky**. Listen over disse programmene er spesifisert som standard og inkludert i programvarepakken for Kaspersky-programmet. Hvis dette alternativet er aktivert, overvåker Kaspersky-programmet alle porter for følgende programmer: • Adobe Acrobat Reader. • Apple Application Support. • Google Chrome. • Microsoft Edge. • Mozilla Firefox. • Internet Explorer. • Java. • mIRC. • Opera. • Pidgin.

	• Safari. • Mail.ru Agent. • Yandex Browser. • **Overvåk alle porter for spesifiserte programmer**. Du kan angi programmene i vinduet **Programmer**, som kan åpnes ved å klikke på **Velg**.
Nettverksporter	En liste over porter som vanligvis brukes ved overføring av e-post og nettrafikk, er inkludert i distribusjonspakken til Kaspersky-programmet. Som standard overvåker Kaspersky-programmet trafikken gjennom alle porter fra denne listen. Du kan legge til porter i listen, eller slette dem fra listen. Hvis verdien *Aktiv* er angitt på portlinjen i **Status**-kolonnen, vil Kaspersky-programmet overvåke trafikken via denne porten. Hvis statusen *Inaktiv* vise på portlinjen i **Status**-kolonnen, utelater Kaspersky-programmet denne porten fra skanninger, men fjerner den ikke fra listen over porter. Du kan endre status og andre portinnstillinger i vinduet ved å klikke på **Rediger**.
Skanning av krypterte tilkoblinger	Du kan velge en av følgende moduser for skanning av krypterte tilkoblinger over SSL: • **Ikke skann krypterte tilkoblinger**. • **Skann krypterte tilkoblinger på forespørsel fra beskyttelseskomponenter**. • **Skann alltid krypterte tilkoblinger**. Hvis alternativet **Skann krypterte tilkoblinger på forespørsel fra beskyttelseskomponenter** er valgt, bruker Kaspersky-programmet det installerte Kaspersky-sertifikatet for å bekrefte sikkerheten til SSL-tilkoblinger hvis dette kreves av beskyttelseskomponentene Sikker surfing og URL-veileder. Hvis disse komponentene er deaktiverte, vil Kaspersky-programmet ikke verifisere sikkerheten til SSL-tilkoblinger. Etter at Kaspersky-programmet verifiserer en SSL-tilkobling, kan det hende at sertifikater for nettsteder ikke viser navnet på organisasjonen nettstedet er registrert hos. Hvis du ikke vil at programmet skal bekrefte en SSL-tilkobling til et nettsted, kan du legge til nettstedet i listen over unntak ved å klikke på lenken **Klarerte adresser**.
Når det oppstår feil med skanning av krypterte forbindelser	I rullegardinmenyen kan du velge handlingen som programmet skal utføre, hvis det oppstår en feil ved skanning av sikre tilkoblinger på nettstedet. • **Ignorer**. Programmet avslutter tilkoblingen med nettstedet hvor skannefeilen oppstod. • **Spør**. Programmet viser en varsling som ber om å legge til en nettstedsadresse i listen over nettsteder hvor det har oppstått skannefeil. Nettstedsadressen vil bli kontrollert mot databasen med skadelige objekter. • **Legg til domenet i unntak**. Programmet legger til nettstedsadressen i listen over nettsteder hvor det har oppstått skannefeil. Nettstedsadressen vil bli kontrollert mot databasen med skadelige objekter.
Domener med skannefeil	Liste over domener som ikke kunne skannes på grunn av feil ved tilkobling til dem. Adressene til domenene ble kontrollert mot databasen med skadelige objekter.
Klarerte adresser	Klikk på denne lenken for å åpne **Klarerte adresser**, som inneholder en liste med

	nettsteder du har lagt til som unntak for komponentene Sikker surfing og URL-veiviser.
Klarerte programmer	Liste over programmer som Kaspersky-programmet ikke overvåker aktiviteten til mens de er i bruk. Du kan velge hvilke programaktiviteter Kaspersky-programmet ikke vil overvåke (ikke skanne nettverkstrafikk, for eksempel). Kaspersky-programmet har støtte for miljøvariabler, og maskene `*` og `?`.
Blokker tilkoblinger via SSL 2.0 (anbefalt)	Hvis dette alternativet er aktivert, blokkerer programmet nettverkstilkoblinger som er opprettet over SSL 2.0-protokollen. Hvis avkrysningsruten er fjernet, vil ikke programmet blokkere nettverkstilkoblinger som er opprettet over SSL 2.0-protokollen, og overvåker ikke nettverkstrafikk som overføres over disse tilkoblingene.
Dekrypter en kryptert tilkobling med nettstedet som bruker EV-sertifikat	EV-sertifikater (Extended Validation Certificates) bekrefter ektheten til nettsteder, og øker sikkerheten til en tilkobling. Nettlesere bruker et hengelåsikon i adresselinjen for å indikere at nettsteder har et EV-sertifikat. Nettlesere kan også farge adresselinjen helt eller delvis grønn. Hvis alternativet er aktivert, vil programmet dekryptere og overvåke krypterte tilkoblinger til nettsteder som bruker et EV-sertifikat. Hvis alternativet er deaktivert, har ikke programmet tilgang til innholdet i HTTPS-trafikk. Programmet overvåker derfor HTTPS-trafikk kun basert på nettadressen, for eksempel `https://bing.com`. Den krypterte tilkoblingen vil bli dekryptert når du åpner et nettsted med et EV-sertifikat for første gang, uavhengig av om alternativet er aktivert eller ikke.
Proxy-serverinnstillinger	Innstillinger for proxy-serveren som brukes til Internett-tilgang for brukere av klientdatamaskiner. Kaspersky-programmet bruker disse innstillingene for visse beskyttelseskomponenter, inkludert for oppdatering av databaser og programmoduler. Kaspersky-programmet bruker WPAD-protokollen (Web Proxy Auto-Discovery Protocol) til å konfigurere en proxy-server automatisk. Hvis proxy-serverens IP-adresse ikke kan fastslås ved hjelp av denne protokollen, bruker programmet proxy-serveradressen som er spesifisert i nettleserinnstillingene for Microsoft Internet Explorer.
Bruk valgt sertifikatlager for å skanne krypterte tilkoblinger i Mozilla-apper	Hvis dette alternativet er valgt, skanner programmet kryptert trafikk i Mozilla-nettleseren Firefox og e-postklienten Thunderbird. Tilgang til enkelte nettsteder via HTTPS-protokollen kan være blokkert. Du må aktivere Skanning av krypterte tilkoblinger for å skanne trafikk i Mozilla Firefox og Thunderbird. Hvis Skanning av krypterte tilkoblinger er deaktivert, skanner ikke programmet kryptert trafikk i Mozilla Firefox og Thunderbird. Programmet bruker Kaspersky-rotsertifikatet til å dekryptere og analysere kryptert trafikk. Du kan velge sertifikatlageret som inneholder Kaspersky-rotsertifikatet. • **Bruk Windows' sertifikatlager (anbefales)**. Kaspersky-rotsertifikatet legges til i dette lageret under installasjon av Kaspersky-programmet. • **Bruk Mozillas sertifikatlager**. Mozilla Firefox og Thunderbird bruker sine egne sertifikatlagere. Hvis Mozillas sertifikatlager er valgt, må du legge til Kaspersky-rotsertifikatet manuelt i dette lageret gjennom nettleserens egenskaper.

Behandle programinnstillinger

Innstillinger	Beskrivelse
Importer	Pakk ut programinnstillinger fra en fil i CFG-format og bruk dem.
Eksporter	Lagre gjeldende programinnstillinger i en fil i CFG-format.
Gjenopprett	Du kan når som helst gjenopprette programinnstillingene som anbefales av Kaspersky. Når innstillingene er gjenopprettet, brukes **Optimalt** sikkerhetsnivå for alle beskyttelseskomponenter.

Innstillinger	Beskrivelse
Varsle om sårbarheter i trådløse nettverk	Hvis avmerkingsboksen er aktivert, viser Kaspersky-programmet varslinger når det oppdages sårbarheter i et trådløse nettverk. Dette alternativet kan velges hvis Kaspersky VPN Secure Connection ikke er installert på datamaskinen. Hvis avmerkingsboksen **Blokker og advar om usikker overføring av passord over Internett** er aktivert, vil Kaspersky-programmet blokkere overføring av passord som ikke-kryptert tekst når du fyller inn **Passord**-felter på Internett. Når du klikker på **Velg kategorier**, åpnes vinduet **Kategorier**, der du kan angi hvilke typer sårbarheter som gjelder for trådløse nettverk. Programmet vil varsle deg når du prøver å koble deg til et trådløst nettverk som har en spesifisert sårbarhet.
Vis enheter som er koblet til nettverkene mine	Hvis avmerkingsboksen er aktivert, er Smart Home Monitor aktivert og funksjonelt.
Tillat tilkoblinger på vilkårlige porter for aktiv FTP-modus	Hvis dette alternativet er valgt, tillater brannmuren tilkoblinger til datamaskinen din på vilkårlige porter hvis et bytte til aktiv FTP-modus ble oppdaget på vertstilkoblingen.
Ikke deaktiver brannmuren før operativsystemet slås av helt	Hvis dette alternativet er valgt, slutter ikke brannmuren å fungere før operativsystemet slås helt av.
Blokker nettverkstilkoblinger hvis brukeren ikke kan bes om handlinger	Hvis avmerkingsboksen er aktivert, stopper ikke Brannmur når grensesnittet til Kaspersky-programmet ikke er lastet inn.
Programregler	Ved å klikke på denne lenken åpnes vinduet **Programnettverksregler**. Dette vinduet viser informasjon relatert til kontroll av nettverksaktiviteten til programmer og programgrupper. Komponenten Inntrengningsbeskyttelse regulerer nettverksaktiviteten til programmer i henhold til nettverksreglene for programmer og programgrupper. Du kan konfigurere tillatelser for nettverksaktivitet i et program eller en programgruppe via menyen til en celle i kolonnen **Nettverk**. Menyelementene er beskrevet i delen Regler for Inntrengningsbeskyttelse. Ved å velge **Detaljer og regler** i hurtigmenyen på en rad, kan du fortsette med å konfigurere nettverksregler for et program eller en programgruppe.
Pakkeregler	Ved å klikke på denne lenken åpnes vinduet **Pakkeregler**. Som standard viser vinduet forhåndsdefinerte nettverkspakkeregler som anbefales av Kaspersky-eksperter for optimal beskyttelse av nettverkstrafikk på datamaskiner med Microsoft Windows. Nettverkspakkeregler innfører begrensninger for nettverkspakker, uavhengig av program. Slike regler begrenser inn- og utgående nettverkstrafikk gjennom bestemte porter i den valgte dataprotokollen. Nettverkspakkeregler har høyere prioritet enn nettverksregler for programmer.

Du kan definere følgende innstillinger når du legger til eller redigerer en pakkeregel:

- Handling:
  - **Tillat**. Kaspersky-programmet tillater nettverkstilkoblingen.
  - **Blokker**. Kaspersky-programmet blokkerer nettverkstilkoblingen.
  - **Etter programregler**. Kaspersky-programmet behandler ikke datastrømmen i henhold til pakkeregelen, men bruker i stedet en programregel (se **Programregler** ovenfor).
- Navn.
- Retning:
  - **Innkommende**. Kaspersky-programmet bruker regelen på nettverkstilkoblinger som åpnes av en ekstern datamaskin.
  - **Utgående**. Kaspersky-programmet bruker regelen på nettverkstilkoblingen som ble åpnet av datamaskinen din.
  - **Innkommende/utgående**. Kaspersky-programmet bruker regelen både på innkommende og utgående datapakker eller -strømmer, uavhengig av hvilken datamaskin (din eller en ekstern datamaskin) som initierte nettverksforbindelsen.
  - **Innkommende (pakke)**. Kaspersky-programmet bruker regelen for datapakker mottatt av datamaskinen.
  - **Utgående (pakke)**. Kaspersky-programmet bruker regelen for datapakker som sendes av datamaskinen.
- Protokoll.
- ICMP-innstillinger. Du kan angi typen og koden til datapakker som skal skannes. Innstillingene er tilgjengelige hvis protokollene ICMP, ICMPv6 er valgt.
- Eksterne porter (porter på en ekstern datamaskin).
- Lokale porter (porter på datamaskinen).

  Du kan angi en rekke eksterne eller lokale porter (for eksempel `6660-7000`), liste opp flere porter atskilt med komma, eller kombinere begge metodene (for eksempel `80-83,443,1080`).

- Adresse:
  - **Vilkårlig adresse**.
  - **Delnettadresser**. Kaspersky-programmet bruker regelen på IP-adressene til alle nettverk som er tilkoblet for øyeblikket og er av den angitte typen (*Offentlig*, *Lokalt* eller *Klarert*). Typen nettverk kan velges fra rullegardinlisten som vises nedenfor hvis alternativet **Delnettadresser** er valgt.

	• **Adresser fra listen**. Kaspersky-programmet bruker regelen på IP-adresser i det angitte området. Du kan angi IP-adresser i feltene **Eksterne adresser** og **Lokale adresser**, som vises nedenfor hvis alternativet **Adresser fra listen** er valgt. IP-adressene som legges til, må være atskilt med komma. • Status. Brannmur gjelder bare for pakkeregler som har statusen **Aktiv**. Du kan sette statusen til **Inaktiv** for å deaktivere en pakkeregel midlertidig, uten å slette den fra listen over pakkeregler. • Nettverkskort som er traversert av nettverkspakker. • Bruk av TTL. Kaspersky-programmet kontrollerer overføringen av nettverkspakker med en levetid (TTL) som ikke overstiger den angitte verdien. • Logger hendelser til rapporten i Kaspersky-programmet. Du kan velge en av de forhåndsdefinerte malene i rullegardinlisten nederst i vinduet for å legge til en regel raskt.
Tilgjengelige nettverk	Klikk på denne koblingen for å åpne vinduet **Nettverk**, som inneholder en liste over nettverkstilkoblinger som brannmuren oppdager på datamaskinen. I listen kan du endre nettverkstypen (*Offentlig*, *Klarert* eller *Lokalt*) ved å bruke menyen i cellen **Nettverkstype** Du kan redigere nettverksinnstillinger i vinduet **Nettverksegenskaper**, som kan åpnes ved å dobbeltklikke på raden i nettverket. Nettverkstypen *Offentlig* er tilordnet til Internett som standard. Du kan ikke endre nettverkstypen eller andre innstillinger for Internett. I vinduet **Nettverksegenskaper** kan du redigere følgende nettverksinnstillinger: • Nettverksnavn. • Nettverkstype. • Visning av varsler om følgende: • Tilkobling til nettverket. • Endret MAC-adresse (for eksempel hvis nettverkskortet byttes ut). • Endret paring av MAC-adresse/IP-adresse (for eksempel når DHCP-tjenesten tilordner en annen IP-adresse). • Valg av skriver som bør anbefales som standard når du kobler til dette nettverket. Denne innstillingen vises hvis en skriver er installert i operativsystemet på datamaskinen. • Liste over ytterligere delnett (atskilt med komma).

Programregler/grupperegler

Innstillinger	Beskrivelse
Fil (kun i vinduet **Programregler**)	Referanseinformasjon om et program og om programmets kjørbare fil. Kaspersky-programmet mottar informasjon om et program fra programmets kjørbare fil og fra Kaspersky Security Network.
Filer og systemregister	Regler for tilgang til systemregisternøkler og filer relatert til bruk av operativsystemet eller de personlige dataene dine. De individuelle tilgangsinnstillingene for lesing, skriving, oppretting og sletting kan defineres hver for seg ved å bruke menyen i cellene i de tilhørende tabellkolonnene. Menyelementene er beskrevet i delen Regler for Inntrengningsbeskyttelse.
Rettigheter	Tilgangsrettigheter til operativsystemressurser og -prosesser, og oppstartsrettigheter. Du kan angi tilgangsrettigheter ved å bruke menyen i cellene i kolonnen **Handling**. Menyelementene er beskrevet i delen Regler for Inntrengningsbeskyttelse.

Nettverksregler	Regler som brukes av Kaspersky-programmet for å regulere nettverksaktiviteten til et program eller en programgruppe.
	Som standard viser listen de forhåndsdefinerte programnettverksreglene som anbefales av Kasperskys eksperter. Du kan ikke slette eller redigere forhåndsdefinerte nettverksregler (bortsett fra å endre handlingen i kolonnen **Tillatelse**. Se beskrivelsen av handlingene som kan brukes, i delen Regler for Inntrengningsbeskyttelse).
	Du kan definere følgende innstillinger når du legger til eller redigerer en regel:
	• Handling:
	  • **Tillat**. Kaspersky-programmet tillater nettverkstilkoblingen.
	  • **Blokker**. Kaspersky-programmet blokkerer nettverkstilkoblingen.
	  • **Spør brukeren**. Hvis alternativet **Utfør anbefalte handlinger automatisk** er deaktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**, spør Kaspersky-programmet om brukeren vil godta eller avslå nettverkstilkoblingen. Hvis alternativet er aktivert, velges handlingen automatisk. Du kan sjekke fotnoten i programvinduet for å lese nøyaktig hvilken handling som blir valgt.
	• Navn.
	• Retning:
	  • **Innkommende**. Kaspersky-programmet bruker regelen på nettverkstilkoblinger som åpnes av en ekstern datamaskin.
	  • **Utgående**. Kaspersky-programmet bruker regelen på nettverkstilkoblingen som ble åpnet av datamaskinen din.
	  • **Innkommende/utgående**. Kaspersky-programmet bruker regelen både på innkommende og utgående datapakker eller -strømmer, uavhengig av hvilken datamaskin (din eller en ekstern datamaskin) som initierte nettverksforbindelsen.
	• Protokoll.
	• ICMP-innstillinger. Du kan angi typen og koden til datapakker som skal skannes. Innstillingene er tilgjengelige hvis protokollene ICMP, ICMPv6 er valgt.

- Eksterne porter (porter på en ekstern datamaskin).
- Lokale porter (porter på datamaskinen).

  Du kan angi en rekke eksterne eller lokale porter (for eksempel `6660–7000`), liste opp flere porter atskilt med komma, eller kombinere begge metodene (for eksempel `80–83,443,1080`).

- Adresse:
  - **Vilkårlig adresse**.
  - **Delnettadresser**. Kaspersky-programmet bruker regelen på IP-adressene til alle nettverk som er tilkoblet for øyeblikket og er av den angitte typen (*Offentlig*, *Lokalt* eller *Klarert*). Typen nettverk kan velges fra rullegardinlisten som vises nedenfor hvis alternativet **Delnettadresser** er valgt.
  - **Adresser fra listen**. Kaspersky-programmet bruker regelen på IP-adresser i det angitte området. Du kan angi IP-adresser i feltet **Ekstern adresse**, som vises nedenfor hvis alternativet **Adresser fra listen** er valgt.
- Nettverkskort som er traversert av nettverkspakker.
- Bruk av TTL. Kaspersky-programmet kontrollerer overføringen av nettverkspakker med en levetid (TTL) som ikke overstiger den angitte verdien.
- Logger hendelser til rapporten i Kaspersky-programmet.

Du kan velge en av de forhåndsdefinerte malene i rullegardinlisten nederst i vinduet for å legge til en regel raskt.

Unntak

(kun i vinduet **Programregler**)

Du kan velge regler som skal brukes for å unnta et program fra skanninger:

- Ikke skann åpnede filer.
- Ikke overvåk programaktivitet. Inntrengningsbeskyttelse overvåker ingen programaktiviteter.
- Ikke arve begrensninger fra den overordnede prosessen (til programmet). Hvis begrensninger for overordnede prosesser eller programmer ikke arves, overvåkes programaktivitet i henhold til reglene du har definert eller i henhold til reglene i klareringsgruppen programmet tilhører.
- Ikke overvåk underordnet programaktivitet.
- Ikke blokker samhandling med grensesnittet til Kaspersky-programmet Programmet tillates å administrere Kaspersky-programmet ved å bruke det grafiske grensesnittet. Du må eventuelt tillate at programmet styrer grensesnittet til Kaspersky-programmet når du bruker et program for tilkobling til eksternt skrivebord eller et program som støtter handlingene til en dataregistreringsenhet. Eksempler på slike enheter omfatter berøringsputer og grafiske nettbrett.
- Ikke skann all trafikk (eller kryptert trafikk). Avhengig av det valgte alternativet (**Ikke skann all trafikk** eller **Ikke skann kryptert nettverkstrafikk**), unntar Kaspersky-programmet all nettverkstrafikk i programmet eller trafikk som overføres via SSL fra å bli skannet. Verdien i denne innstillingen påvirker ikke brannmuren: Den skanner

	programtrafikk i henhold til innstillingene for brannmuren. Unntak påvirker E-post-Antivirus, Sikker surfing og Anti-Spam. Du kan angi IP-adressene eller nettverksportene begrensningen for trafikkontroll må gjelde for.
Historikk (kun i vinduet **Programregler**)	Referanseinformasjon om handlinger som utføres på programmet, for eksempel å starte programmet eller tildele en klareringsgruppe.

Regler for Inntrengningsbeskyttelse

En *regel* er et sett med reaksjoner fra Inntrengningsbeskyttelse, som svar på handlingene et program kjører på forskjellige kategorier av operativsystemressurser og personlige data.

Inntrengningsbeskyttelse kan reagere på handlinger fra et program på følgende måter:

- **Arv**. Inntrengningsbeskyttelse reagerer på programmets aktivitet ved å bruke regelen som er konfigurert for statusen som Inntrengningsbeskyttelse har tilordnet til programmet.

  Denne reaksjonen brukes som standard. Som standard arver Inntrengningsbeskyttelse tilgangsrettigheter fra statusen som Inntrengningsbeskyttelse har tilordnet til programmet.

  Hvis du redigerte en regel for et program, vil regelen for programmet ha høyere prioritet enn regelen for statusen som ble tilordnet til programmet.

- **Tillat**. Inntrengningsbeskyttelse tillater programmet å utføre handlingen.

- **Nekt**. Inntrengningsbeskyttelse hindrer programmet i å utføre handlingen.

- **Spør brukeren**. Hvis alternativet **Utfør anbefalte handlinger automatisk** er deaktivert under **Innstillinger** → **Ytelsesinnstillinger** → **PC-ressursforbruk**, ber Inntrengningsbeskyttelse brukeren om å velge. Hvis alternativet er aktivert, velges handlingen automatisk. Du kan sjekke fotnoten i vinduet i Kaspersky-programmet for å lese nøyaktig hvilken handling som blir valgt.

- **Logg hendelser**. Inntrengningsbeskyttelse loggfører informasjon om programmets aktivitet og svarene på den i en rapport. Informasjon kan legges til en rapport sammen med andre handlinger Inntrengningsbeskyttelse har utført.

Innstillinger for Sikkert datainput

Innstillinger	Beskrivelse
Bruk virtualisering av maskinvare hvis det er tilgjengelig	Hvis avkrysningsboksen er valgt, brukes maskinvarevirtualisering (hypervisor) for driften av Beskyttet nettleser. Programmet bruker hypervisorteknologi for ytterligere beskyttelse mot komplisert skadelig programvare som kan fange opp dine personlige data ved hjelp av utklippstavlen eller såkalt phishing. Denne avmerkingsboksen vises hvis programmet er installert på en 64-biters versjon av Windows 8, Windows 8.1 eller Windows 10. For flere detaljer om maskinvarevirtualisering og hvordan det fungerer, kan du klikke på koblingen.
Beskyttelse ved hjelp av virtualisering av maskinvare	Sikkert tastaturinput hjelper deg med å hindre nettkriminelle i å snappe opp dataene du taster inn fra tastaturet når du besøker nettsteder (se delen Om Sikkert tastaturinput for mer informasjon). Merk av i boksene for kategoriene med nettsteder der du vil beskytte inntasting av data via tastaturet. Klikk på **Behandle unntak** for å lage lister over nettsteder du vil aktivere eller deaktivere Sikkert tastaturinput på, uavhengig av de valgte nettstedkategoriene. Du kan bruke masker når du legger til unntak.
Skjermtastatur	Mange programmer som er klassifisert som spionprogrammer, kan ta skjermbilder og automatisk sende disse til en inntrenger, som vil analysere dem og stjele brukerens personlige data. Skjermtastatur beskytter personlige data som skrives inn, mot oppfangingsforsøk ved hjelp av skjermbilder. (se Om skjermtastatur for mer informasjon). Du må starte datamaskinen på nytt etter at du har installert Kaspersky-programmet for å være sikker på at skjermtastaturet er aktivert. Du kan velge hvordan skjermtastaturet åpnes: • **Åpne Virtuelt tastatur med tastekombinasjonen CTRL+ALT+SHIFT+P**. • **Vis ikonet for hurtigoppstart i dataregistreringsfelter**. Hurtigstartikonet for skjermtastaturet vises i inntastingsfeltene for passord på nettsider. Merk av i boksene for kategoriene med nettsteder der du vil beskytte inntasting av data via skjermtastaturet. Klikk på **Behandle unntak** i vinduet **Unntak for skjermtastatur** for å lage lister over nettsteder du vil aktivere eller deaktivere visning av hurtigstartikonet for skjermtastaturet på, uavhengig av nettstedskategoriene som er valgt. Du kan bruke masker når du legger til unntak.
Vis hint for hvordan du lager sterke passord	Hvis dette alternativet er aktivert, vil Kaspersky-programmet kontrollere styrken på et passord du angir i nettleseren for første gang, og varsle deg om det.
Beskyttelse mot bruk av de samme passordene	Når du angir et passord på et nettsted der et sikkert passord er spesielt viktig (f.eks. på et sosialt nettverk), ber Kaspersky-programmet deg om å aktivere beskyttelse mot bruk av identiske passord. Hvis alternativet **Advar om bruk av samme passord på nettsteder** er valgt, er beskyttelse mot bruk av samme passord aktivert. Du kan **velge nettstedkategorier** som skal beskyttes mot å bruke de samme passordene. Disse kategoriene inkluderer nettstedene til banker og betalingssystemer, sosiale nettverk og e-posttjenester. Klikk på **Slett lagrede data** for å slette alle tidligere lagrede passord.

Vinduet Velg filer som skal slettes

Felt for å skrive inn banen til filen eller mappen

Feltet inneholder banen til en fil eller mappe som skal slettes permanent. Du kan velge en fil eller en mappe fra treet over registreringsfeltet eller angi den manuelt.

Vinduet Velg data for kryptering

Felt for å skrive inn banen til filen eller mappen

Dette feltet inneholder banen til filen eller mappen som skal legges til i et hemmelig hvelv. Du kan velge en fil eller en mappe fra treet over registreringsfeltet eller angi den manuelt.

Vindu for åpning av hemmelig hvelv

Passord for å åpne det hemmelige hvelvet

Passord for tilgang til filer i det hemmelige hvelvet

Åpne i Windows Utforsker

Når du klikker på denne knappen, åpnes en mappe med en liste over filer og mapper som er lagret i det hemmelige hvelvet, i Windows Utforsker.

Vindu for sletting av hemmelig hvelv

Passord for å åpne det hemmelige hvelvet

Passord for tilgang til filer i det hemmelige hvelvet

Slett hemmelig hvelv

Når du klikker på denne knappen, vil Kaspersky-programmet slette det hemmelige hvelvet og alle filene som er lagret i hvelvet.

Filene og mappene i det hemmelige hvelvet slettes permanent.

Vindu for å gi nytt navn til hemmelig hvelv

Nytt navn på hvelvet

Det nye navnet som skal tilordnes det hemmelige hvelvet.

Lagre

Når du klikker på denne knappen, vil Kaspersky-programmet tilordne det nye navnet til datahvelvet.

Vinduet Endre passord for hemmelig hvelv

Gammelt passord

Gjeldende passord for hemmelig hvelv.

Nytt passord

Nytt passord for hemmelig hvelv.

Bekreft passord

Tast inn passordet du har angitt i feltet **Nytt passord** på nytt.

Lagre

Klikk på denne knappen for å erstatte det gjeldende passordet for det hemmelige hvelvet med det nye passordet.

Velg fil eller hemmelig hvelv-vindu

Felt for å skrive inn banen til filen

Feltet inneholder banen til det hemmelige hvelvet. Du kan velge et hemmelig hvelv fra treet over registreringsfeltet, eller angi banen til det hemmelige hvelvet manuelt.

Vinduet Sikkerhetskopiering og gjenoppretting

Velg filer

Denne knappen starter veiviseren for oppretting av sikkerhetskopieringsoppgaver.

Gjenopprette filer fra sikkerhetskopisettet mitt

Når du klikker på denne koblingen, åpnes et vindu med en liste over sikkerhetskopilagre. I dette vinduet kan du velge et lager som inneholder et eldre sett med sikkerhetskopier.

Knappene ◻ / ⏸ / ▷

Knappene kan brukes til å styre sikkerhetskopieringen:

◻ – Stoppe en sikkerhetskopiering. Denne knappen vises hvis en sikkerhetskopiering kjører eller er stoppet midlertidig.

⏸ – Pause en sikkerhetskopiering. Denne knappen vises hvis en sikkerhetskopiering kjører.

▷ – Starte en sikkerhetskopiering eller gjenoppta en sikkerhetskopiering som er stanset midlertidig. Knappen er tilgjengelig hvis en sikkerhetskopiering er fullført eller er stanset midlertidig.

Kjør

Når du klikker på knappen, startes prosessen som oppretter sikkerhetskopier av filer. Denne knappen vises kun hvis ingen sikkerhetskopieringer kjører.

Klikk på ⌄-knappen for å åpne en meny der du kan velge flere handlinger for de angitte innstillingene for sikkerhetskopiering:

- **Endre innstillinger** – starter redigeringsveiviseren for sikkerhetskopieringsinnstillinger.
- **Slett innstillinger** – Sletter sikkerhetskopieringsinnstillinger.

Gjenopprett filer

Denne knappen åpner vinduet **Gjenopprett filer fra sikkerhetskopier**. I dette vinduet kan du velge sikkerhetskopiene du vil gjenopprette filer fra.

Logg på Dropbox

Når du klikker på denne knappen, åpnes påloggingsvinduet for Dropbox-nettstedet. Hvis du ikke har noen konto, kan du registrere deg på nettstedet til Dropbox.

Knappen vises hvis du ikke har logget på nettstedet til Dropbox fra denne datamaskinen enda.

Oppdater status

Når du klikker på denne knappen, vil Kaspersky-programmet koble til det nettbaserte lageret og oppdatere informasjonen om størrelsen på det nettbaserte lageret og størrelsen på filene i lageret.

Denne knappen vises hvis programmet ikke kunne hente informasjon om det nettbaserte lageret (for eksempel hvis datamaskinen ikke var tilkoblet Internett) tidligere.

detaljer

Ved å klikke på denne lenken åpnes vinduet **Rapporter**. Dette vinduet viser detaljert informasjon om fullførte sikkerhetskopieringer.

Kjøremodus

Ved å klikke på denne lenken åpnes vinduet **Tidsplan for sikkerhetskopiering**. I dette vinduet kan du endre kjøremodusen for sikkerhetskopieringen.

Rydd opp

Denne knappen åpner vinduet **Rydd opp i lager**, der du kan fjerne uønskede sikkerhetskopier fra sikkerhetskopilageret.

Opprett sikkerhetskopier av andre filer

Når du klikker på denne knappen, åpnes vinduet til Veiviseren for oppretting av sikkerhetskopieringsoppgave, der du kan legge til filer som skal sikkerhetskopieres.

Gjenopprett filer fra sikkerhetskopier som ikke finnes i listen

Ved å klikke på denne lenken åpnes vinduet **Søk etter sikkerhetskopier**. I dette vinduet kan du angi et sikkerhetskopilager som allerede inneholder opprettede sikkerhetskopier.

Behandle lagre

Klikk på denne knappen for å åpne et vindu med en liste over tilgjengelige sikkerhetskopilagre. I dette vinduet kan du gjenopprette filer fra sikkerhetskopier i det valgte lageret, redigere innstillingene til det valgte lageret, slette dette lageret eller legge til et lager i listen.

Vinduet Velg mappe som skal sikkerhetskopieres

Felt for å skrive inn banen til mappen

Feltet inneholder banen til mappen som skal sikkerhetskopieres. Du kan velge en mappe fra treet over registreringsfeltet eller angi den manuelt.

Vinduet Gjenopprettingsverktøy

Kopier Kaspersky Restore Utility til lager

Hvis alternativet er aktivert, kopieres Kasperskys gjenopprettingsverktøy til lageret under sikkerhetskopieringen. Dette verktøyet kan brukes til å gjenopprette filer fra sikkerhetskopier hvis Kaspersky-programmet er skadet eller ikke installert.

Vinduet Filer valgt for sikkerhetskopiering

Liste over filtyper

Inneholder navnene på alle filtypene og antall filer av hver type.

Når et listeelement er valgt, vises alle filer av denne typen.

Liste over filer av valgt filtype

Inneholder informasjon om filer av en bestemt type, som er valgt for sikkerhetskopiering: filnavn, plassering og størrelse.

Hvis avmerkingsboksen ved siden filnavnet er aktivert, sikkerhetskopierer programmet denne filen.

Hvis avmerkingsboksen ved siden filnavnet er deaktivert, sikkerhetskopierer ikke programmet denne filen.

Delen Nettverksstasjon

Disk

Banen til en nettverksmappe som brukes som sikkerhetskopilager.

Bla gjennom

Denne knappen åpner vinduet **Velg mappe**. I dette vinduet kan du velge en nettverksmappe som skal brukes som sikkerhetskopilager.

Brukernavn

Navnet på kontoen som gir tilgang til nettverksmappen. Brukernavnet må angis i formatet *<datamaskinnavn>\<brukernavn>* (for eksempel *kl-12345\ivanov*).

Passord

Passordet som gir tilgang til nettverksmappen.

Delen Lokal stasjon

Liste over lokale stasjoner

Listen inneholder de lokale stasjonene på datamaskinen. Du kan velge en av de lokale stasjonene som lager for sikkerhetskopier.

Hvis den lokale stasjonen ikke vises på listen, kan du angi banen til denne stasjonene i feltet nedenfor. Du kan også klikke på **Bla gjennom**, og velge den lokale stasjonen i vinduet **Velg mappe for sikkerhetskopiering** som åpnes.

Bla gjennom

Denne knappen åpner vinduet **Velg mappe for sikkerhetskopiering**. I dette vinduet kan du velge en lokal stasjon som brukes som sikkerhetskopilager.

Delen Flyttbar stasjon

Liste over tilkoblede flyttbare stasjoner

Listen inneholder flyttbare stasjoner som er koblet til datamaskinen. Du kan velge en av de flyttbare stasjonene som lager for sikkerhetskopier.

Hvis den flyttbare stasjonen ikke vises på listen, kan du angi banen til denne stasjonene i feltet nedenfor. Du kan også klikke på **Bla gjennom**, og velge den flyttbare stasjonen i vinduet **Velg mappe** som åpnes.

Bla gjennom

Denne knappen åpner vinduet **Velg mappe**. I dette vinduet kan du velge en flyttbar stasjon som brukes som sikkerhetskopilager.

Delen Nettbasert lager

Hvis du vil bruke Nettbasert lager, logger du på nettstedet dropbox.com. Når du klikker på **OK**, åpnes en nettside med påloggingsvinduet for dropbox.com.

Vinduet Lagre

Liste over lagre

Viser en liste over opprettede sikkerhetskopilagre. Informasjonen som vises for hvert lager, omfatter total og brukt lagringsplass, plassering av lager, oppgaver som bruker dette lageret og tilgjengelige handlinger.

Gjenopprett filer

Klikk på denne knappen for å åpne et vindu med sikkerhetskopisett som er laget på dette lageret. I dette vinduet kan du velge et sett med sikkerhetskopier du vil gjenopprette filer fra.

Klikk på -knappen for å åpne en meny der du kan velge en annen handling:

- **Endre innstillinger** – Starter redigeringsveiviseren for lagringsinnstillinger.
- **Slett lager** – Den valgte stasjonen eller nettressursen brukes ikke lenger som lager for sikkerhetskopier, og alle sikkerhetskopier slettes fra lageret.
- **Rydd opp i lager** – åpner vinduet **Rydd opp i lager**. I dette vinduet kan du velge sikkerhetskopier som skal fjernes fra lageret for å frigjøre lagringsplass.

Legg til nettverkslager

Ved å klikke på denne lenken åpnes vinduet **Legg til nettverkslager**. I dette vinduet kan du angi innstillingene til en nettverksstasjon som du vil legge til i listen over lager.

Koble til eksisterende lager

Ved å klikke på denne lenken åpnes vinduet **Koble til lager**. I dette vinduet kan du angi innstillingene for lokale stasjoner, flyttbare stasjoner, nettverksstasjoner eller nettbaserte lagre som du vil legge til i listen over lager.

Et vindu som inneholder en liste over sikkerhetskopisett i lageret

Liste over sikkerhetskopisett

Inneholder informasjon om sikkerhetskopisett i lageret:

- Navnet på sikkerhetskopisettet
- Diskplassen som kreves for å gjenopprette filer fra dette settet

Gjenopprett filer

Denne knappen åpner vinduet **Gjenopprett filer fra sikkerhetskopier**. I dette vinduet kan du velge sikkerhetskopiene du vil gjenopprette filer fra.

Vinduet Støtte

Delen **Kasperskys tekniske støtte** inneholder informasjon som er nødvendig når du kontakter Kasperskys tekniske støttetjeneste: versjonsnummer for Kaspersky Small Office Security, utgivelsesdato- og klokkeslett for databaser og programmoduler, operativsystemversjon og lisensnøkkel.

Lisensnøkkel

Klikk på koblingen **<nøkkel>** for å åpne vinduet **Lisensdetaljer**, der du finner informasjon om den aktive lisensen.

Andre versjoner

Ved å klikke på denne lenken åpnes nettstedet der du kan laste ned programversjonen som er beregnet for bruk i din region. Dette trinnet er ikke tilgjengelig i alle versjoner av programmet.

Svar på vanlige spørsmål

Klikk på denne koblingen for å åpne siden for interaktiv støtte i et nettleservindu. Denne side gir svar på vanlige spørsmål som brukerne stiller ekspertene i teknisk støtte hos Kaspersky.

Tips om konfigurasjon av programmet

Når du klikker på denne koblingen, åpnes nettstedet til Teknisk støtte, som viser artikler om hvordan du konfigurerer og bruker Kaspersky.

Fellesskap

Når du klikker på denne knappen, åpnes nettleseren på siden til Kasperskys fellesskap, der du kan se innsendte tråder, legge igjen kommentarer, opprette nye emner og søke etter informasjon.

Støtteverktøy

Når du klikker på denne koblingen, åpnes vinduet **Støtteverktøy**. I dette vinduet kan du samle inn teknisk informasjon om programmets drift og opprette en systemstatusrapport.

Vinduet Rydd opp i lager

Sikkerhetskopier opprettet tidligere enn

En funksjon som fjerner sikkerhetskopiene av filene som er opprettet før datoen angitt i feltet ved siden av avmerkingsboksen, fra lageret.

Tidligere versjoner av sikkerhetskopier

Hvis denne avmerkingsboksen er valgt, slettes gamle versjoner av sikkerhetskopier når du rydder opp i sikkerhetskopilageret. Antall nylige sikkerhetskopiversjoner som skal beholdes, er angitt i feltet **Antall versjoner av sikkerhetskopier som skal beholdes**.

Sikkerhetskopier av filer som de opprinnelige filene er slettet for

Dette alternativet aktiverer/deaktiverer en funksjon som fjerner kopier av filer som er slettet på datamaskinen, fra sikkerhetskopilageret.

Vinduet Velg sikkerhetskopiversjonen du vil gjenopprette

Liste over sikkerhetskopiversjoner

Inneholder informasjon om tilgjengelige versjoner av sikkerhetskopier av filen. Hvert listeelement viser filnavn, versjonsnummer og sikkerhetskopiversjonens opprettelsesdato.

Når du høyreklikker et listeelement, åpnes en hurtigmeny med følgende elementer:

- **Åpne** – versjonen av sikkerhetskopien av filen åpnes i vinduet til programmet som svarer til filformatet.
- **Gjenopprett sikkerhetskopiversjon** – Vinduet **Velg hvor du vil plassere gjenopprettede filer** åpnes. I dette vinduet kan du velge mappen der du vil lagre den gjenopprettede filen.

Gjenopprett

Klikk på denne knappen for å åpne et vindu der du kan endre innstillinger for å gjenopprette filer.

Vinduet Velg mappe

Felt for å skrive inn banen til mappen

Feltet inneholder banen til mappen som filene skal gjenopprettes i. Du kan velge en mappe fra treet over registreringsfeltet, eller angi banen til mappen manuelt.

Vinduet Gjenopprett filer

Stopp

Når du klikker på denne knappen, vil Kaspersky-programmet stoppe gjenoppretting av filer fra sikkerhetskopier.

Vinduet Gjenopprettet fil finnes allerede

Erstatt filen med sikkerhetskopien

Kaspersky-programmet sletter den eksisterende filen og erstatter den med filen som er gjenopprettet fra sikkerhetskopien.

Ikke gjenopprett denne filen

Kaspersky-programmet lar den eksisterende filen være uendret, og gjenoppretter ikke filen fra filen med samme navn fra sikkerhetskopien.

Lagre begge filene

Kaspersky-programmet lar den eksisterende filen være uendret, og lagrer filen som er gjenopprettet fra sikkerhetskopien, under et annet navn i samme mappe.

Bruk denne handlingen på alle liknende tilfeller

Hvis dette alternativet er aktivert, bruker Kaspersky-programmet den valgte handlingen på alle filer som gjenopprettes.

Vinduet Gjenopprett filer

Stopp

Når du klikker på denne knappen, vil Kaspersky-programmet stoppe gjenoppretting av filer fra sikkerhetskopier.

Vinduet Lagerinnstillinger

Navn på lager

Feltet inneholder navnet på et sikkerhetskopilager.

Vinduet Kaspersky Restore Utility

Sikkerhetskopiering

Du kan velge data som skal gjenopprettes fra denne rullegardinlisten.

Dato/klokkeslett for sikkerhetskopiering

Fra denne rullegardinlisten kan du velge datoen og klokkeslettet da filene du vil gjenopprette, ble sikkerhetskopiert. De valgte filene gjenopprettes til versjonene på dette tidspunktet.

Søk

Et felt der du kan søke etter sikkerhetskopien til en fil basert på navnet. Søket starter straks du begynner å skrive inn bokstavene.

Knappen  /

Denne vekslebryteren endrer visningen av listen over sikkerhetskopier: mappetre eller liste over filer sortert alfabetisk.

Filliste

Listen inneholder sikkerhetskopier av filer som kan gjenopprettes.

Posisjonen til vekslebryteren  bestemmer om vinduet skal vise et mappe tre eller en liste med alle sikkerhetskopiene sortert alfabetisk.

Denne listen viser informasjon om navnet på sikkerhetskopien, plasseringen til kildefilen, filtypen, filformatet, filstørrelsen og antall sikkerhetskopier av denne filen. Hvis du klikker i kolonnen **Versjon**, åpnes vinduet **Velg sikkerhetskopiversjonen du vil gjenopprette**. I dette vinduet kan du velge hvilken versjon av en sikkerhetskopi filen skal gjenopprettes fra.

Hvis avmerkingsboksen ved siden av en sikkerhetskopi er aktivert, gjenoppretter programmet denne filen.

Hvis avmerkingsboksen ved siden av en sikkerhetskopi er deaktivert, gjenoppretter ikke programmet denne filen.

Når du høyreklikker et listeelement, åpnes en hurtigmeny med følgende elementer:

- **Åpne fil** – filen åpnes med programmet som er ment for håndtering av filer av denne typen.
- **Gjenopprett siste versjon av sikkerhetskopien** – åpner vinduet **Velg hvor du vil plassere gjenopprettede filer**, der du kan angi en målmappe for gjenoppretting av den nyeste versjonen av filens sikkerhetskopi.
- **Versjoner av sikkerhetskopier av fil** – Vinduet **Velg sikkerhetskopiversjonen du vil gjenopprette** åpnes. I dette vinduet kan du velge hvilken versjon av en sikkerhetskopi filen skal gjenopprettes fra.

Versjon

Klikk på denne koblingen for å åpne vinduet **Velg sikkerhetskopiversjonen du vil gjenopprette**, der du kan vise alle versjoner av den valgte filen som kan gjenopprettes.

Velg et annet lager

Klikk på denne knappen for å åpne vinduet vor valg av sikkerhetskopilager.

Gjenopprett valgte data

Klikk på denne knappen for å åpne et vindu der du kan endre innstillinger for å gjenopprette filer.

Bruke Foreldrekontroll

Med *Foreldrekontroll* kan du overvåke handlingene som utføres av brukere på den lokaledatamaskinen og på Internett. Foreldrekontroll kan brukes til å begrense tilgang til Internett-ressurser og programmer, samt til å vise rapporter med brukeraktiviteter.

I dag har stadig flere barn og tenåringer tilgang til datamaskiner og webressurser. Økt bruk av datamaskiner og Internett har ført til en rekke nye farer for barn:

- Sløsing av tid og/eller penger ved besøk til chatterom, spillressurser, nettbutikker og auksjoner
- Tilgang til nettsteder som er beregnet på et voksent publikum og for eksempel inneholder pornografi, ekstremisme, skytevåpen, narkotikamisbruk og eksplisitt vold
- Nedlasting av filer som er infisert med skadelig programvare
- Helseskader forårsaket av overdrevet datamaskinbruk
- Kontakt med fremmede som later som om de er like gamle, for å oppnå opplysninger fra brukeren, for eksempel navn og adresse, når ingen er hjemme

Med Foreldrekontroll kan du redusere risikoene ved datamaskinbruk og Internett-bruk. Det gjør du ved å bruke følgende funksjoner til å:

- Begrense datamaskin- og Internett-bruk
- Opprette lister over tillatte og blokkerte spill, samt midlertidig begrense bruk av tillatte programmer
- Opprette lister over tillatte og blokkerte nettsteder og blokkere kategorier med nettsteder som har uegnet innhold
- Aktivere sikker søkemodus for søkemotorer (koblinger til nettsteder med mistenkelig innhold vises ikke i søkeresultatene)
- Begrense nedlasting av filer fra Internett
- Blokkere sending av visse personlige data

Du kan konfigurere funksjonene i Foreldrekontroll individuelt for hver brukerkonto på datamaskinen. Hvis en bruker bruker to kontoer, for eksempel en lokal konto for operativsystemet og en Microsoft-brukerkonto, skal innstillingene for Foreldrekontroll konfigureres for Microsoft-brukerkontoen.

Du kan også vise rapporter om aktivitetene til overvåkede brukere i Foreldrekontroll.

Når tidssonen endres, eller når du bytter til og fra sommertid, gjelder følgende regler for bruk av datamaskinen og Internett, samt for å starte spill og programmer:

- Hvis datoen ikke endres når tidssonen endres, fortsetter den nåværende nedtellingen til blokkering uten endringer. Samme regel gjelder når du bytter til eller fra sommertid.
- Hvis datoen hopper frem eller tilbake når tidssonen endres, nullstilles brukerens tid og nedtellingen til blokkering begynner igjen.

Fortsette til innstillingene i Foreldrekontroll

Slik går du til innstillingene for Foreldrekontroll:

1. Åpne hovedvinduet.
2. Gå til delen **Sikkerhet**.
3. I blokken **Foreldrekontroll** klikker du på **Aktiver**-knappen.
4. Hvis tilgang til Foreldrekontroll ikke er passordbeskyttet, vil programmet be brukeren om å angi et passord. Velg ett av følgende alternativer:

   - Slik beskytter du tilgang til foreldrekontrollinnstillingene med et passord:

     a. Fyll ut feltene **Passord** og **Bekreft passord** og klikk på **Fortsett**.

     b. Gå til vinduet **Passordomfang** og klikk på **Opprett passord**.

     c. I vinduet **Skriv inn passord** bekrefter du passordet og klikker på **Logg på**.

   - Hvis du ikke vil passordbeskytte innstillingene for Foreldrekontroll, klikker du på koblingen **Hopp over** for å fortsette til innstillingene for Foreldrekontroll.

   Vinduet **Foreldrekontroll** åpnes.

5. Velg en brukerkonto og klikk på koblingen **Konfigurer begrensninger** for å åpne innstillingsvinduet i Foreldrekontroll.

Kontrollere datamaskinbruk

Foreldrekontroll kan brukes til å begrense tiden som brukeren tilbringer ved datamaskinen. Du kan angi et tidsintervall når Foreldrekontroll skal blokkere tilgang til datamaskinen (sengetid), samt en generell tidsbegrensning for datamaskinbruk hver dag. Du kan angi ulike tidsverdier for ukedager og helger.

Slik konfigurerer du tidsbegrensning på datamaskinbruk:

1. Gå til Innstillingsvinduet i Foreldrekontroll.
2. Velg delen **Datamaskin** i innstillingsvinduet i Foreldrekontroll.
3. Hvis du vil angi et tidsintervall der Foreldrekontroll skal blokkere tilgangen til datamaskinen, går du til **Ukedager** og **Helger** og merker av for **Blokker tilgang fra N til N**.
4. Angi tidspunktet for blokkeringsoppstart i rullegardinlisten ved siden av boksen **Blokker tilgang fra N**.
5. Angi tidspunktet for blokkeringsstopp i rullegardinlisten **til N**.

   Foreldrekontroll vil blokkere brukerens tilgang til datamaskinen under det angitte tidsintervallet.
6. Du kan opprette tidsplanen for datamaskinbruk ved hjelp av en tabell. Hvis du vil se tabellen, klikker du på -knappen.

   Foreldrekontroll vil blokkere brukerens tilgang til datamaskinen **etter tidsplan** som spesifisert i tabellen.
7. Hvis du vil begrense den totale datamaskinbruken i løpet av én dag, merker du av for alternativet **Ikke tillat tilgang i mer enn N timer per dag** i delene **Ukedager** og **Helger**. Deretter velger du et tidsintervall i rullegardinlisten ved siden av avmerkingsboksen.

   Foreldrekontroll blokkerer brukerens tilgang til datamaskinen når den samlede datamaskinbruken i løpet av en dag overstiger den angitte tiden.
8. Hvis du vil legge inn pauser i brukerens datamaskinøkter, går du til delen **Pauser** og merker av for **Ta en pause <time> for <duration>**. Deretter velger du verdier for pausenes hyppighet (for eksempel hver time) og lengde (for eksempel 10 minutter) i rullegardinlisten ved siden av avmerkingsboksen.
9. Skyv vekselbryteren øverst i vinduet til **Kontroll er aktivert** .

Foreldrekontroll vil blokkere brukerens tilgang til datamaskinen i henhold til de angitte innstillingene.

Kontrollere Internett-bruk

Med Foreldrekontroll kan du begrense tiden som brukes på Internett og forby at brukere får tilgang til bestemte kategorier med nettsteder eller angitte nettsteder. Dessuten kan du forby at brukeren laster ned filer av bestemte typer (for eksempel arkiver eller videoer) fra Internett.

Slik begrenser du brukstid for Internett

Slik setter du tidsbegrensninger for bruk av Internett:

1. Gå til Innstillingsvinduet i Foreldrekontroll.
2. Velg delen **Internett** i innstillingsvinduet i Foreldrekontroll.
3. Hvis du vil begrense den samlede tiden på Internett på ukedager, velger du **Begrens tilgang på ukedager til N timer per dag** i delen **Begrensning av Internett-tilgang**, og velger deretter en verdi for tidsbegrensningen i rullegardinlisten ved siden av alternativet.
4. Hvis du vil begrense den samlede tiden på Internett i helgene, velger du alternativet **Begrens tilgang i helger til N timer per dag**, og velger deretter en verdi for tidsbegrensningen i rullegardinlisten ved siden av alternativet.
5. Skyv vekselbryteren øverst i vinduet til **Kontroll er aktivert** .

Foreldrekontroll vil begrense brukerens totale Internett-bruken i henhold til verdiene du har angitt.

Slik begrenser du besøk på bestemte nettsteder

Slik begrenser du besøk på bestemte nettsteder:

1. Gå til Innstillingsvinduet i Foreldrekontroll.
2. Velg delen **Internett** i innstillingsvinduet i Foreldrekontroll.
3. Hvis du vil unngå at nettsteder med innhold for voksne vises i søkeresultater, går du til delen **Kontroller nettsurfing** og merker av for alternativet **Aktiver Sikkert søk for søkemotorer**.

   Når du søker etter informasjon på nettsteder som Google™, YouTube™ (kun for brukere som ikke har logget inn på youtube.com under egen konto), Bing®, Yahoo!™ og Yandex, vil ikke noe seksuelt innhold vises i søkeresultatene.
4. Slik blokkerer du tilgang til nettsteder i bestemte kategorier:
   a. Gå til delen **Kontroller nettsurfing** og merk av for alternativet **Kontroller tilgang til nettsteder**.
   b. Velg alternativet **Blokker tilgang til nettsteder fra valgte kategorier** og klikk på koblingen **Velg kategorier med nettsteder** for å åpne vinduet **Blokker tilgang til nettstedkategorier**.
   c. Aktiver avmerkingsboksene ved siden av kategoriene til nettsteder som skal blokkeres.

      Foreldrekontroll vil blokkere alle brukerens forsøk på åpne et nettsted hvis innholdet er klassifisert i en av de blokkerte kategoriene.
5. Slik blokkerer du tilgang til bestemte nettsteder:
   a. Gå til delen **Kontroller nettsurfing** og merk av for alternativet **Kontroller tilgang til nettsteder**.
   b. Klikk på koblingen **Behandle unntak** for å åpne vinduet **Unntak**.
   c. Klikk på **Legg til** nederst i vinduet.

      Et vindu for å legge til en ny nettadressemaske åpnes.
   d. Angi adressen på nettstedet du vil blokkere, ved å fylle ut feltet **Nettadressemaske**.
   e. I delen **Omfang** definerer du omfanget på det du vil blokkere: hele nettstedet eller bare den angitte nettsiden.
   f. Hvis du vil blokkere det angitte nettstedet, går du til delen **Handling** og velger **Blokker**.
   g. Klikk på **Legg til**.

   Det angitte nettstedet vises på listen i vinduet **Unntak**. Lukk vinduet **Unntak**.
6. Skyv vekselbryteren øverst i vinduet til **Kontroll er aktivert**  .

Foreldrekontroll vil blokkere forsøk på å åpne nettsteder i henhold til de angitte innstillingene.

Slik blokkerer du nedlasting av bestemte typer filer

Slik blokkerer du nedlasting av bestemte filtyper fra Internett:

1. Gå til Innstillingsvinduet i Foreldrekontroll.
2. Velg delen **Internett** i innstillingsvinduet i Foreldrekontroll.
3. I delen **Blokker filnedlasting** merker du av avkrysningsboksene ved siden av filtyper du vil blokkere nedlasting av.
4. Skyv vekselbryteren øverst i vinduet til **Kontroll er aktivert** .

Foreldrekontroll vil blokkere nedlasting av filer av bestemte typer fra Internett.

Kontrollere oppstart av spill og programmer

Ved hjelp av Foreldrekontroll kan du tillate og forby at brukeren starter spill avhengig av deres aldersrangering. Du kan også forhindre brukeren i å starte spesifiserte programmer (som spill eller IM-klienter) eller begrense tiden som er tillatt for å bruke programmer.

Slik blokkerer du spill med innhold som er uegnet for barn

Blokkere spill med innhold som er uegnet for alderen:

1. Gå til Innstillingsvinduet i Foreldrekontroll.
2. I innstillingsvinduet i Foreldrekontroll velger du delen **Programmer**.
3. Hvis du vil blokkere alle spill med innhold som er uegnet for brukerens alder, merker du av for **Begrens oppstart av spill for brukere som er yngre enn**. Deretter velger du et alternativ for aldersbegrensning i rullegardinlisten ved siden av avmerkingsboksen.
4. Hvis du vil blokkere spill med innhold fra en bestemt kategori:
   a. Merk av for alternativet **Blokker spill fra voksne kategorier**.
   b. Klikk på koblingen **Velg kategorier med spill** for å åpne vinduet **Blokker spill etter kategorier**.
   c. Aktiver avmerkingsboksene ved siden av innholdskategoriene som matcher spillene du vil blokkere.
5. Gå tilbake til delen **Programmer**.
6. Hvis du vil bruke rangeringssystemet til å blokkere spill, velger du type rangering og innholdskategorisering i rullegardinlisten **Bruk dette rangeringssystemet til å blokkere spill**:
   - **Slett automatisk** – Foreldrekontroll velger type spillrangering basert på hvor du er: innholdsrangeringssystemet PEGI (Pan European Game Information) eller rangeringssystemet for USA og Canada (ESRB).
   - **PEGI** – Foreldrekontroll bruker det europeiske rangeringssystemet til å konfigurere tillatelser til å starte spill.
   - **ESRB** – Foreldrekontroll bruker rangeringssystemet for USA og Canada til å konfigurere tillatelser til å starte spill.
7. Skyv vekselbryteren øverst i vinduet til **Kontroll er aktivert**.

Slik begrenser du oppstart av et bestemt program

Slik begrenser du oppstart av et bestemt program:

1. Gå til Innstillingsvinduet i Foreldrekontroll.
2. I innstillingsvinduet i Foreldrekontroll velger du delen **Programmer**.
3. Klikk på koblingen **Konfigurer** for å åpne vinduet **Programbruk**.
4. Klikk på **Legg til program** for å åpne vinduet **Åpne** og velge programmets kjørbare fil.

   Det valgte programmet vises i listen **Programbruk**. Kaspersky llegger automatisk til dette programmet i en bestemt kategori, for eksempel *Spill*.
5. Utfør følgende handlinger:

   - Velg elementet **Blokker** i rullegardinlisten ved siden av programnavnet hvis du vil blokkere oppstart av programmet.
   - Du kan blokkere alle programmer som tilhører en bestemt kategori, ved å velge avmerkingsboksen ved siden av navnet på den aktuelle kategorien i listen (du kan for eksempel blokkere programmer i kategorien *Spill*).
   - Velg elementet **Tillat** i rullegardinlisten ved siden av programnavnet hvis du vil tillate oppstart av programmet.
   - Hvis du vil angi begrensninger for hvor lenge et program kan brukes, velger du elementet **Begrens** i rullegardinlisten til høyre for programnavnet.

     Vinduet **Begrensing av programbruk** åpnes.

     Utfør følgende handlinger:

     a. Hvis du vil angi en tidsbegrensning for bruk av et program på ukedager og i helgene, merker du av for alternativet **Ikke tillat tilgang i mer enn <N> timer per dag** i delene **Ukedager** og **Helger**. Deretter angir du antall timer per dag som brukeren kan bruke programmet på, i rullegardinlisten. Du kan også angi når brukeren har lov til eller ikke lov til å bruke programmet, ved hjelp av tabellen **Nøyaktig brukstid**.

     b. Hvis du vil angi perioder når programmet er satt på pause, merker du av for alternativet **Ta en pause <time> for <interval>** i delen **Pauser** og velger verdier for hvor hyppig og hvor lenge intervallet må være.

     c. Klikk på **Lagre**.
6. Lukk vinduet **Programbruk**.
7. Skyv vekselbryteren øverst i vinduet til **Kontroll er aktivert** .

   Foreldrekontroll bruker de angitte begrensningene når brukeren håndterer programmet.

Overvåke meldingsinnhold

Med Foreldrekontroll kan du overvåke og forby brukerens forsøk på å sette inn bestemte personlige data (for eksempel navn, telefonnumre, bankkortnumre) i meldinger.

Slik konfigurerer du kontroll av overføring av personlige data

Slik konfigurerer du kontroll av overføring av personlige data:

1. Gå til Innstillingsvinduet i Foreldrekontroll.
2. Velg delen **Innholdskontroll** i innstillingsvinduet i Foreldrekontroll.
3. I delen **Kontroll av overføring av personlige data** merker du av for alternativet **Blokker overføring av personlige data til tredjeparter**.
4. Klikk på koblingen **Rediger liste over personlige data** for å åpne vinduet **Liste over personlige data**.
5. Klikk på **Legg til** nederst i vinduet.

   Et vindu der du kan legge til personlige data, åpnes.
6. Velg typen med personlige data (for eksempel telefonnummer) ved å klikke på den aktuelle koblingen eller legg inn en beskrivelse i feltet **Feltnavn**.
7. Angi personlige data (for eksempel etternavn eller telefonnummer) i feltet **Verdi**.
8. Klikk på **Legg til**.

   De personlige dataene du har lagt til, vil vises i vinduet **Liste over personlige data**.
9. Lukk vinduet **Liste over personlige data**.
10. Skyv vekselbryteren øverst i vinduet til **Kontroll er aktivert** .

    Foreldrekontroll overvåker og blokkerer brukerens forsøk på å bruke angitte personlige data i meldingsutvekslinger på Internett.

Vise rapporten om brukeraktivitet

Du får tilgang til rapportene om brukerkontoenes aktiviteter under Foreldrekontroll, der hver kategori av kontrollerte hendelser kan gjennomgås separat.

Hvis du vil vise en rapport om aktivitetene til en kontrollert brukerkonto:

1. Gå til Innstillingsvinduet i Foreldrekontroll.
2. Velg en brukerkonto og klikk på koblingen **Vis rapport** for å gå til rapportvinduet.
3. I delen med ønsket type begrensninger (for eksempel **Internett**) åpner du rapporten over overvåkede handlinger ved å klikke på koblingen **Detaljer**.

Vinduet viser en rapport over brukerens overvåkede handlinger.

Vinduet Nettstedkategorier

Internettbanker og betalingssystemer

Hvis dette alternativet er aktivert, vil programmet vise et varsel hvis du oppretter eller angir et passord på Internett som du har brukt tidligere på nettstedene til banker og betalingssystemer.

Sosiale nettverk

Hvis dette alternativet er aktivert, viser programmet et varsel hvis du oppretter eller angir et passord på Internett som du har brukt tidligere på sosiale nettverk.

E-posttjenester

Hvis dette alternativet er aktivert, vil programmet vise et varsel hvis du oppretter eller angir et passord på Internett som du har brukt tidligere på nettstedene til e-posttjenester.

Hjelp oss til å bli bedre! Vinduet Gi oss tilbakemeldinger

Parametersettet i dette vinduet avhenger av vurderingen du ga komponenten. Parameteren Problemkategori er tilgjengelig hvis du ga komponenten en vurdering på 1 til 2.

Emne

En rullegardinliste der du kan velge en kategori for tilbakemeldingene dine. Tilbakemeldingskategori kan løse et problem med komponenten Smart Home Monitor.

- **Upraktisk å bruke**. Velg dette elementet hvis du opplever ulemper når du bruker komponenten Smart Home Monitor.
- **Programmet bruker for lang tid til å søke etter enheter i nettverket**. Velg dette elementet hvis komponenten Smart Home Monitor jobber for sakte.
- **Programmet identifiserer enheter i nettverket feil**. Velg dette elementet hvis programmet feilaktig bestemmer navnene på og/eller typene enheter som er koblet til nettverket.
- **For mange varsler om nye enheter i nettverket**. Velg dette elementet hvis programmet viser deg for mange varsler om nye enheter på nettverket.
- **Redusert PC-ytelse**. Velg dette elementet hvis bruken av komponenten Smart Home Monitor reduserer datamaskinens ytelse.
- **Kan ikke konfigurere komponenten**. Velg dette elementet hvis du opplever problemer når du konfigurerer komponenten Smart Home Monitor.
- **Annet**. Velg dette elementet hvis problemet du opplever ikke dekkes av andre elementer.

Detaljer

Du kan bruke dette feltet til å oppgi informasjon som kan hjelpe Kaspersky med å løse problemet. Dette feltet er valgfritt.

Send

Sende tilbakemeldingen til Kaspersky

Du kan sende tilbakemeldinger om komponenten Smart Home Monitor opptil 10 ganger per dag. Hvis programmet ikke kan sende tilbakemeldingen (for eksempel fordi du ikke har internettforbindelse), lagres tilbakemeldingen på datamaskinen. Den lagrede tilbakemeldingen vil være synlig i 30 dager.

Om Lisensavtale for sluttbrukere

Lisensavtalen for sluttbrukere er en bindende avtale mellom deg og AO Kaspersky Lab, som angir vilkårene for bruk av programmet.

Les vilkårene i lisensavtalen nøye før du begynner å bruke programmet.

Du må bekrefte at du godtar vilkårene i Lisensavtalen når du installerer programmet. Hvis du ikke godtar vilkårene i Lisensavtalen, må du avbryte installasjonen av programmet, og kan ikke bruke programmet.

Om modusen begrenset funksjonalitet

Tabellen nedenfor viser hvilke funksjoner i Kaspersky-programmet som er tilgjengelige og ikke tilgjengelige når programmet kjører i modusen for begrenset funksjonalitet. Hvis verdien i kolonnen Modus for begrenset funksjonalitet er Ja, betyr det at den aktuelle funksjonen er tilgjengelig i denne modusen. Hvis verdien i Modus for begrenset funksjonalitet er Nei, er den aktuelle funksjonen ikke tilgjengelig. Du vil se tilleggsinformasjon i kolonnen Begrensninger.

Kaspersky-programmets funksjoner i modus for begrenset funksjonalitet

Funksjon	Begrensninger	Modus for begrenset funksjonalitet
Virusskann		ja
Oppdatere antivirusdatabaser og programmoduler	Bare kritiske oppdateringer er tilgjengelige.	nei
Sårbarhetsskanning av programmer		ja
Sikker surfing		ja på Windows 7, 8 / nei på Windows 10, 11
Fil-Antivirus		ja på Windows 7, 8 / nei på Windows 10, 11
E-post-Antivirus		ja på Windows 7, 8 / nei på Windows 10, 11
Systemvakt		ja på Windows 7, 8 / nei på Windows 10, 11
Sjekker omdømmet til filer i Kaspersky Security Network		nei
Sikkert datainput		nei
Nødgjenoppretting	Kaspersky Rescue Disk kan lastes ned i programgrensesnittet.	ja
Trusler og unntak		ja
Nettverksinnstillinger		ja
Rapporter og karantene		ja
Programvisningsinnstillinger		ja
Spillmodus		nei
Ikke forstyrr-modus		nei
Inntrengningsbeskyttelse		ja på Windows 7, 8 / nei på Windows 10, 11
Brannmur		ja
Nettverkangrepsblokkering		ja
Anti-Spam		ja
Anti-Banner		ja
Safe Money		nei
Privat surfing		ja

Personvernrengjøring		nei
Smart Home Monitor		nei
Webkamera og mikrofonkontroll		ja på Windows 7, 8 / nei på Windows 10, 11
Nettverksovervåker		ja
Application Manager		nei
Password Manager		ja
Filmakulering		ja
Hemmelig hvelv	Kun tilgang til data i tidligere opprettede hemmelige hvelv, er tilgjengelig.	nei
Sikkerhetskopiering og gjenoppretting	Kun gjenoppretting av data fra sikkerhetskopier du har opprettet tidligere, er tilgjengelig.	nei
Programoppdatering		nei
PC-renser		nei
PC Speed-Up		nei
Kaspersky VPN		ja
Datalekkasjekontroll		nei
Feilsøking av Microsoft Windows		ja
Rask oppstart		nei
Skann for svake innstillinger		nei
Duplikater		nei
Store filer		nei
Ubrukte programmer		nei
Overvåking av harddiskens helse		nei
Gjeldende aktivitet		nei
Batterisparer		nei
Stalkerware-deteksjon		nei
Blokkering av installasjon av uønskede programmer		nei
Fjerning av annonseprogrammer		nei
AMSI-beskyttelse		ja, bare på Windows 10, 11
Behandle innstillinger		ja
Passordbeskyttelse for programinnstillinger		ja
Innstillinger for PC-ressursforbruk		ja

Historikk		ja
Anbefalinger		ja
Foreldrekontroll	Bare rapportvisning er tilgjengelig.	nei
Kontakte Teknisk støtte		ja

Om phishing

Phishing er en form for svindel på Internett som omfatter tyveri av personopplysninger. Phishing spres via e-post og andre kanaler.

Disse e-postene kan være falske meldinger fra banker, Internett-leverandører, nettbutikker, elektroniske betalingssystemer eller andre instanser. E-postene forsøker å lure mottakeren til å besøke svindlernes nettsted under falske forutsetninger, for eksempel informasjon om at de må oppdatere påloggingsinformasjon eller en invitasjon til å finne ut mer om et produkt eller en tjeneste.

Hvis intetanende mottakere av phishingforsøk via e-post følger lenken, kommer de til et phishing-nettsted som ser ut helt likt ut som nettstedet til selskapet e-postens avsender utgir seg for å være fra.

Internett-brukere kan komme til et phishing-nettsted på andre måter, for eksempel ved å klikke på en lenke i en søkemotor.

Svindlere kan ha en rekke forskjellige mål med dette. Et av disse målene er å lure brukere til å dele konfidensielle opplysninger, for eksempel påloggingsdetaljer, passord til kontoer eller kryptolommebøker og andre registreringsdata, bankkontonumre og bankkortdetaljer. Brukere som legger inn denne informasjonen i et nettskjema på svindlernes phishing-nettsted, kan ende opp med å gi svindlerne tilgang til pengene sine. Å få datamaskinene infisert med virus og skadelig programvare er en annen felle en bruker kan gå i etter å ha klikket på en phishing-lenke.

Gjenkjenne bedragerske e-poster og nettsteder

Bedragerske e-poster og nettsteder (phishing) kan se umistenkelige ut ved første øyekast. Inkludering av firmalogoer som ser autentiske ut, eller ekte kontakttelefonnumre, kan gi brukerne en falsk følelse av sikkerhet. E-posten kan også inneholde lenker til selskapets faktiske nettsted, i tillegg til phishing-lenken som omdirigerer brukeren til de kriminelles nettsted.

Her er noen tydelige tegn på phishing som brukeren kan oppdage:

- Selv om domenene til phishing-nettsteder kan se ut som selskapenes faktiske domener, kan brukeren inspisere dem nøyere for å legge merke til ekstra ord i domenenavnet (for eksempel kan et selskaps offisielle domene www.example.com være endret til www.login-example.com), eller prikker og bindestreker som erstatter skråstreker (www.example.com/personal/login kan være endret til www.example.com.personal.login eller www.example.com-personal.login). Vær oppmerksom på at teksten i e-posten kan inneholde selskapets faktiske domene, men når brukeren klikker på lenken, vil nettleserens adresselinje vise et annet domene.

- E-posten bruker en upersonlig adresseform, for eksempel «Kjære bruker» eller «Hei».

- Grafikken i e-posten eller på nettsiden ser uprofesjonell ut, teksten inneholder skrivefeil eller dårlig grammatikk.

- E-postmottakeren blir bedt om å umiddelbart bekrefte konfidensiell informasjon ved å følge en lenke, eller noen ganger skrive inn informasjonen sin i et skjema i e-postteksten. E-posten kan fortelle at det haster, med påstander suspendering av kontoen eller hacking, eller en trussel om å miste data.

Phishing-sjekk

Kaspersky-programmet sjekker e-post- og nettstedinnhold for phishing-koblinger. Lenker sjekkes mot en database med phishing-nettadresser og falske kryptobørser, som oppdateres jevnlig.

For ytterligere beskyttelse under phishing-sjekker bruker Kaspersky heuristisk analyse og sender forespørsler til de skybaserte tjenestene til Kaspersky Security Network (KSN). Kaspersky Security Network har den mest oppdaterte informasjonen om nylig oppståtte trusler, inkludert phishing-nettsteder som ennå ikke er lagt til Kaspersky-databaser. Dataene som mottas av KSN analyseres av Virus Lab-ansatte i sanntid.

Hvis du har klikket deg inn på et phishing-nettsted, kan du rapportere det til Kaspersky Security Network ved å bruke utvidelsen for Kaspersky Protection.

Profil

Koble en enhet til My Kaspersky

Du trenger en My Kaspersky-konto for å administrere abonnementet, aktivere abonnementet på forskjellige enheter og fjernstyre beskyttelsen av slike enheter. På My Kaspersky-kontoen kan du se statusen til alle enheter som er koblet til kontoen, hvis programmet installert på dem. Du kan også administrere abonnementer og lagre aktiveringskoder på et trygt sted.

Logg på

Klikk på denne knappen for å åpne et vindu der du kan koble enheten til My Kaspersky-kontoen din. Knappen er tilgjengelig hvis du ikke har koblet enheten til My Kaspersky-kontoen din enda, eller hvis du ikke har bekreftet at enheten er din.

Avhengig av abonnementet ditt, kan det hende at enkelte funksjoner i programmet ikke er tilgjengelige hvis ikke du har koblet enheten til My Kaspersky-kontoen din.

Administrer konto

Hvis du klikker på denne knappen, omdirigeres du til kontoen din på nettstedet til My Kaspersky i standardnettleseren. Knappen blir tilgjengelig etter at du har logget på kontoen på denne enheten.

Knappen

Klikk på denne knappen for å koble enheten fra My Kaspersky-kontoen din. Knappen er tilgjengelig hvis enheten er koblet til My Kaspersky-kontoen din.

Avhengig av abonnementet ditt kan det være nødvendig å koble enheten til My Kaspersky-kontoen din. Du vil ikke kunne bruke programmet etter at du har koblet enheten fra kontoen din.

Mer om My Kaspersky-kontoen

Abonnementsdetaljer

Her finner du generell informasjon om abonnementet som brukes av programmet ditt. Du kan se statusen til abonnementet, antall dager som gjenstår til den betalte perioden utløper, status for automatisk fornyelse og navnet til abonnementets eier hvis du ikke er eieren.

Detaljer

Klikk på denne knappen for å åpne vinduet **Abonnementsdetaljer**, som viser detaljert informasjon om abonnementet. Her finner du følgende informasjon:

- Abonnementsstatus
- Status for automatisk fornyelse
- Lisensnøkkel som du kan trenge for å kontakte teknisk støtte
- Lenke til lisensavtalen for sluttbrukere
- Lenke til nettportalerklæringen
- Totalt antall enheter du kan beskytte med abonnementet ditt
- Antall enheter du for øyeblikket beskytter med abonnementet ditt
- Aktiveringsdato
- Utløpsdato for den betalte perioden

Klikk på ••• for å se hvilke andre handlinger du kan gjøre med abonnementet ditt. Listen over tilgjengelige handlinger avhenger av abonnementet og abonnementets status, og kan derfor være annerledes.

Oppdater status

Klikk på denne knappen for å få oppdatert informasjon om statusen til abonnementet ditt.

Skriv inn aktiveringskode

Klikk på denne knappen for å åpne vinduet der du kan skrive inn aktiveringskoden. Det er ikke sikkert at du vil se denne knappen, da det kommer an på abonnementet ditt.

Du finner mer informasjon om aktiveringskoder i delene Hvis du har kjøpt en boks eller et aktiveringskort og Fornye abonnementet med en reserve-aktiveringskode.

Velge et annet abonnement

Når du klikker på denne knappen, åpnes et vindu med en liste over tilgjengelige abonnementer i My Kaspersky-kontoen som er kompatible med programmet ditt.

Knappen er tilgjengelig hvis enheten er koblet til My Kaspersky-kontoen din.

Administrer abonnement

Når du klikker på denne knappen, åpnes My Kaspersky-kontoen din og tar deg til siden for administrering av abonnementet. Knappen er tilgjengelig hvis enheten er koblet til My Kaspersky-kontoen din.

Forny nå / kjøp nå

Avhengig av statusen til det gjeldende abonnementet ditt, kan du enten fornye det eller kjøpe et nytt abonnement.

Knappen er tilgjengelig hvis abonnementet ditt er utløpt, forutsatt at du ikke har aktivert automatisk fornyelse ikke har lagt til en reserve-aktiveringskode for programmet.

Gjenoppta

Knappen er tilgjengelig hvis du har sagt opp abonnementet. Du vil kunne gjenoppta abonnementet i en periode etter at du har sagt det opp.

Å gjenoppta det nåværende abonnementet er kanskje ikke tilgjengelig i regionen din.

Mer informasjon om administrering av abonnementet

Beskytt flere enheter

Her kan du se hvor mange enheter du kan beskytte med abonnementet ditt og hvor mange enheter du beskytter for øyeblikket. Du kan også begynne å beskytte nye enheter. Hvis du har koblet en enhet til My Kaspersky-kontoen din, oppdateres informasjonen når du kjører programmet.

Antall enheter du kan bruke abonnementet på avhenger av abonnementet og vilkårene og betingelsene i lisensavtalen for sluttbrukere.

Knappen +

Når du klikker på denne knappen, åpnes vinduet **Beskytt flere enheter** der du kan velge foretrukket metode for å sende abonnementet til enheten.

Knappen er tilgjengelig hvis abonnementet lar deg beskytte mer enn én enhet.

Det er ikke sikkert at denne knappen vises, da det kommer an på abonnementet ditt.

Klikk på ••• -knappen for å velge en av følgende handlinger:

Beskytt enhet

Når du klikker på denne knappen, åpnes vinduet **Beskytt flere enheter** der du kan velge foretrukket metode for å sende abonnementet til en annen enhet.

Knappen er tilgjengelig hvis abonnementet lar deg beskytte mer enn én enhet.

Administrer enheter

Når du klikker på denne knappen, åpnes My Kaspersky-kontoen din og tar deg til siden for administrering av abonnementet i delen **Mine enheter**. Her kan du se alle enhetene som bruker abonnementet ditt, og overvåke statusen til disse enhetene.

Hvis du ikke har koblet en enhet til My Kaspersky-kontoen din enda, åpnes vinduet der du kan koble enheter til kontoen din.

Se hjelpedelen for My Kaspersky for mer informasjon om fjernstyring av enheter.

Avhengig av abonnementet ditt kan det hende at det bare vises generell informasjon om det totale antallet enheter du kan beskytte.

Mer informasjon om beskyttelse av andre enheter med abonnementet ditt

Løsninger for deg

På denne siden vil vi tilby Kaspersky-løsninger og løsninger levert av partnere våre, som du kan kanskje synes er interessant. Her vil du kunne kjøpe en løsning som er skreddersydd for dine behov, bla gjennom tidligere kjøpte applikasjoner og tjenester, holde øye med abonnementsstatusen din, fortsette med å installere et program eller lese en bruksanvisning.

Ved å klikke på **Kjøp**, blir du videreført til nettbutikken, hvor du kan lære mer om løsningen du valgte, i tillegg til å sjekke ut kjøpet ditt. Du vil motta en e-post med informasjon om kjøpet ditt, samt instrukser om aktivering.

Du kan administrere abonnementene du har kjøpt via My Kaspersky-kontoen din.