F-Secure Internet Security 2013

Innhold

Kapitel 1: Installering.....5

Før du installerer for første gang.....6
Installere produktet første gang.....6
Installere og oppgradere programmer.....6
Hjelp og støtte.....7

Kapitel 2: Komme i gang.....9

Hvordan bruke automatiske oppdateringer.....10
Kontrollere oppdateringsstatusen.....10
Endre innstillingene for Internett-tilkobling.....10
Sjekke statusen for sanntidsbeskyttelsesnettverket.....11
Hvordan se hva produktet har gjort.....11
Vise varslingshistorikk.....11
Endre varslingsinnstillingene.....11
Sanntidsbeskyttelsesnettverk.....12
Hva er sanntidsbeskyttelsesnettverket.....12
Fordeler ved sanntidsbeskyttelsesnettverket.....12
Hvilke data du bidrar med.....13
Hvordan vi beskytter personvernet.....14
Bli en bidragsyter til sanntidsbeskyttelsesnettverket.....14
Spørsmål om Sanntidsbeskyttelsesnettverk.....14
Hvordan vet jeg at abonnementet mitt er gyldig.....15
Handlingssenter.....15
Aktivere et abonnement.....15

Kapitel 3: Innledning.....17

Vis den generelle statusen for beskyttelsen.....18
Vise produktstatistikken.....18
Håndtere produktoppdateringene.....19
Vise databaseversjoner.....19
Endre innstillingene for mobilt bredbånd.....19
Hva er virus og annen skadelig programvare.....20
Virus.....20
Spionprogrammer.....20
Rootkits.....21
Risikoprogrammer.....21

Kapitel 4: Beskytte datamaskinen mot skadelig programvare.....23

Hvordan skanne datamaskinen.....24
Skanne filer automatisk.....24
Skanne filer manuelt.....26
Skanne e-postmeldinger.....29
Vise skanneresultatene.....29
Hvordan ekskludere filer fra skanningen.....30
Ekskludere filtyper.....30
Ekskludere filer etter plassering.....31
Vise ekskluderte programmer.....31
Hvordan bruke karantenen.....32
Vise elementer i karantene.....32
Gjenopprette elementer i karantene.....32
Hva er DeepGuard.....33
Slå DeepGuard på eller av.....33
Tillat programmer som DeepGuard har blokkert.....33
Bruke DeepGuard i kompatibilitetsmodus.....34
Hva du bør gjøre med varsler om mistenkelig virkemåte.....34
Hva er en brannmur.....35
Slå brannmuren på eller av.....35
Endre brannmurinnstillinger.....35
Hindre programmer i å laste ned skadelige filer.....36
Blokkere søppelpost.....36
Slå søppelpost- og phishing-filtrering på eller av.....36
Beskytte mot phishing-forsøk.....37
Konfigurere e-postprogrammet til å filtrere vekk søppelpost.....37

Kapitel 5: Sikker bruk av Internett.....39

Hvordan kjøre vanlige oppgaver.....40
Slik beskytter du forskjellige brukerkontoer.....40
Opprette og redigere Windows-brukerkontoer.....40
Hva er nettleserbeskyttelse.....40
Hvordan slå nettleserbeskyttelse på eller av.....40
Sikkerhetsvurderinger i Nettleserbeskyttelse.....41
Beskytte mot skadelig innhold.....42
Hva når et nettsted er blokkert.....42
Sikkerhetssammendrag for et nettsted.....42
Gjøre nettbruk sikker.....43
Begrense tilgang til Internett-innhold.....43
Hvordan angi surfetid.....44
Begrense daglig surfetid.....44
Vise statistikk.....45

Kapitel

1

Installering

Emner:

- *Før du installerer for første gang*
- *Installere produktet første gang*
- *Installere og oppgradere programmer*
- *Hjelp og støtte*

Før du installerer for første gang

Takk for at du velger F-Secure.

Når du skal installere produktet, trenger du følgende:

- Installerings-CDen eller en installeringspakke. Hvis du bruker en netbook uten CD-stasjon, kan du laste ned installeringspakken fra *www.f-secure.com/netbook*.
- Abonnementsnøkkelen din.
- En Internett-tilkobling.

Hvis du har et sikkerhetsprodukt fra en annen leverandør, vil installereren automatisk prøve å fjerne det. Hvis dette ikke skjer, må du fjerne det manuelt.

Merk: Hvis du har mer enn én konto på datamaskinen, må du logge på med administratorrettigheter når du skal installere.

Installere produktet første gang

Instruksjoner for installering av produktet.

Følg disse instruksjonene for å installere produktet:

1. Sett inn CDen eller dobbeltklikk på installeringsprogrammet du lastet ned.

   Hvis CDen ikke starter automatisk, går du til Windows Utforsker, dobbeltklikker på CD-ikonet og dobbeltklikker på setup.exe-filen for å starte installeringen.

2. Følg instruksjonene på skjermen.

   - Hvis du kjøpte produktet på en CD i en butikk, finner du abonnementsnøkkelen på omslaget til installeringsveiledningen.
   - Hvis du lastet ned produktet fra F-Secure eStore, finner du abonnementsnøkkelen i bekreftelsesmeldingen til innkjøpsordren.

   Datamaskinen må kanskje startes på nytt før validering av abonnementet og nedlasting av de nyeste oppdateringene fra Internett. Hvis du installerer fra CDen, må du huske på å ta ut CDen før du omstarter datamaskinen.

Installere og oppgradere programmer

Instruksjoner for aktivering av ditt nye abonnement.

Følg disse instruksjonene når du skal aktivere det nye abonnementet eller installere et nytt program ved å bruke startrampen:

Merk: Du finner startrampeikonet i systemfeltet på oppgavelinjen i Windows.

1. Høyreklikk på ikonet helt til høyre på startrampen.
   Det åpnes en popup-meny.
2. Velg **Vis mine abonnementer**
3. Under **Mine abonnementer** går du til siden **Abonnementsstatus** og klikker på **Aktiver abonnement**.
   Vinduet **Aktiver abonnement** åpnes.

4. Skriv inn abonnementsnøkkelen for programmet, og klikk på **OK**.
5. Når abonnementet er validert og aktivert, klikker du på **Lukk**.
6. Under **Mine abonnementer** går du til siden **Installeringsstatus**. Hvis installeringen ikke starter automatisk, følger du disse instruksjonene:
   a) Klikk på **Installer**.
   Installeringsvinduet åpnes.
   b) Klikk på **Neste**.
   Programmet lastes ned, og installeringen starter.
   c) Når installeringen er fullført, klikker du på **Lukk**.

Det nye abonnementet har blitt aktivert.

Hjelp og støtte

Du åpner produktets elektroniske hjelp ved å klikke på Hjelp-ikonet eller trykke på F1 i et skjermbilde i produktet.

Når du har registrert lisensen, er du berettiget til tilleggstjenester som gratis produktoppdateringer og produktstøtte. Du kan registrere på *www.f-secure.com/register*.

Kapitel

2

Komme i gang

Emner:

- *Hvordan bruke automatiske oppdateringer*
- *Hvordan se hva produktet har gjort*
- *Sanntidsbeskyttelsesnettverk*
- *Hvordan vet jeg at abonnementet mitt er gyldig*

Informasjon om hvordan du kommer i gang med å bruke produktet.

Dette avsnittet beskriver hvordan du endrer felles innstillinger og administrerer abonnementene dine gjennom startrampen.

Fellesinnstillingene på startrampen er innstillinger som gjelder for alle programmene som er installert på startrampen. I stedet for å endre innstillingene for hvert enkelt program, kan du ganske enkelt redigere fellesinnstillingene, som deretter brukes av alle de installerte programmene.

Fellesinnstillingene på startrampen inkluderer:

- Nedlastinger, der du kan se informasjon om hvilke oppdateringer som har blitt lastet ned, og manuelt kontrollere om det er nye oppdateringer tilgjengelig.
- Tilkoblingsinnstillinger, der du kan endre måten datamaskinen kobler til Internett på.
- Varsler, der du kan vise de siste varslene og angi hvilken type varsler du vil se.
- Personverninnstillinger, der du kan velge om datamaskinen kan koble til sanntidsbeskyttelsesnettverket eller ikke.

Du kan også håndtere abonnementer på installerte programmer gjennom startrampen.

Hvordan bruke automatiske oppdateringer

Automatiske oppdateringer holder beskyttelsen på datamaskinen oppdatert.

Produktet henter de siste oppdateringene til datamaskinen din når du er koblet til Internett. Det registrerer trafikken på nettverket og forstyrrer ikke annen Internett-bruk, selv ikke når nettverksforbindelsen er langsom.

Kontrollere oppdateringsstatusen

Vis dato og klokkeslett for siste oppdatering.

Når automatiske oppdateringer er slått på, henter produktet de siste oppdateringene automatisk når du er koblet til Internett.

Slik kontrollerer du at du har de siste oppdateringene:

1. Høyreklikk på ikonet helt til høyre på startrampen.
   Det vises en popup-meny.
2. Velg **Åpne fellesinnstillinger**.
3. Velg **Automatiske oppdateringer** > **Nedlastinger**.
4. Klikk på **Kontroller nå**.
   Produktet kobler til Internett og ser etter de siste oppdateringene. Hvis beskyttelsen ikke er oppdatert, hentes de siste oppdateringene.

   Merk: Hvis du bruker modem eller ISDN for å koble deg til Internett, må tilkoblingen være aktiv for at du skal kunne kontrollere om definisjonene er oppdatert.

Endre innstillingene for Internett-tilkobling

Det er vanligvis ikke nødvendig å endre standardinnstillingene, men du kan konfigurere måten serveren er koblet til Internett på slik at du kan motta oppdateringer automatisk.

Slik endrer du innstillingene for Internett-tilkobling:

1. Høyreklikk på ikonet helt til høyre på startrampen.
   Det vises en popup-meny.
2. Velg **Åpne fellesinnstillinger**.
3. Velg **Automatiske oppdateringer** > **Tilkobling**.
4. På listen **Tilkobling**velger du hvordan datamaskinen kobles til Internett.
   - Velg **Anta at alltid tilkoblet** hvis du har en permanent nettverkstilkobling.

     Merk: Hvis datamaskinen ikke har en permanent nettverkstilkobling og er konfigurert for oppringning ved behov, kan valg av **Anta at alltid tilkoblet** føre til flere oppringninger.
   - Velg **Oppdag tilkobling**for bare å hente oppdateringer når produktet oppdager en aktiv nettverkstilkobling.
   - Velg **Oppdag trafikk** for bare å hente oppdateringer når produktet oppdager annen nettverkstrafikk.

     Tips: Hvis du har en uvanlig maskinvarekonfigurasjon som får innstillingen **Oppdag tilkobling** til å oppdage en aktiv nettverkstilkobling selv om det ikke finnes noen, velger du **Oppdag trafikk** i stedet.
5. På listen **HTTP-proxy** velger du om datamaskinen bruker en *proxyserver* for å koble til Internett.
   - Velg **Ingen HTTP-proxy** hvis datamaskinen kobles til Internett direkte.

- Velg **Konfigurer HTTP-proxy manuelt** for å konfigurere *HTTP-proxy*-innstillingene.
- Velg **Bruk min nettleserens HTTP-proxy** for å bruke de samme *HTTP-proxy*-innstillingene som er konfigurert i nettleseren.

Sjekke statusen for sanntidsbeskyttelsesnettverket

Mange produktfunksjoner er avhengig av tilkobling til sanntidsbeskyttelsesnettverket for å fungere riktig.

Hvis det er nettverksproblemer, eller hvis brannmuren blokkerer trafikk til sanntidsbeskyttelsesnettverket, er statusen "frakoblet". Hvis det ikke er installert noen produktfunksjoner som krever tilgang til sanntidsbeskyttelsesnettverket, er statusen "ikke i bruk".

Slik sjekker du statusen:

1. Høyreklikk på ikonet helt til høyre på startrampen.
   Det vises en popup-meny.
2. Velg **Åpne fellesinnstillinger**.
3. Velg **Automatiske oppdateringer** > **Tilkobling**.

Under **Sanntidsbeskyttelsesnettverk** kan du se gjeldende status for sanntidsbeskyttelsesnettverket.

Hvordan se hva produktet har gjort

Du kan se hvilke handlinger produktet har utført for å beskytte datamaskinen, på **Varsler**-siden.

Produktet vil vise et varsel når det utfører en handling, for eksempel når det finner et virus som blir blokkert. Enkelte varsler kan også bli sendt av tjenesteleverandøren, for eksempel for å la deg få vite om nye tjenester som er tilgjengelig.

Vise varslingshistorikk

Du kan se hvilke varsler som har blitt vist, i varslingshistorikken.

Slik viser du varslingshistorikken:

1. Høyreklikk på ikonet helt til høyre på startrampen.
   Det vises en popup-meny.
2. Velg **Åpne fellesinnstillinger**.
3. Velg **Annet** > **Varsler**.
4. Klikk på **Vis varslingshistorikk**.
   Listen med varslingshistorikk åpnes.

Endre varslingsinnstillingene

Du kan velge hvilken type varsler du vil at produktet skal vise.

Slik endrer du varslingsinnstillingene:

1. Høyreklikk på ikonet helt til høyre på startrampen.
   Det vises en popup-meny.
2. Velg **Åpne fellesinnstillinger**.
3. Velg **Annet** > **Varsler**.
4. Velg eller opphev valget av **Tillat programmeldinger** for å slå programmeldinger på eller av.
   Når denne innstillingen er slått på, vil produktet vise varsler fra programmene som er installert.

5. Velg eller opphev valget av **Tillat reklamemeldinger** for å slå reklamemeldinger på eller av.
6. Klikk på **OK**.

Sanntidsbeskyttelsesnettverk

Dette dokumentet beskriver sanntidsbeskyttelsesnettverket, som er en elektronisk tjeneste fra F-Secure Corporation som identifiserer rene programmer og nettsteder samtidig som det beskytter mot skadelige programmer og nettstedsutnyttere.

Hva er sanntidsbeskyttelsesnettverket

Sanntidsbeskyttelsesnettverket er en elektronisk tjeneste som gir rask respons på nye Internett-baserte trusler.

Som bidragsyter til sanntidsbeskyttelsesnettverket kan du hjelpe oss med å styrke beskyttelsen mot nye og voksende trusler. Sanntidsbeskyttelsesnettverket samler inn statistikk over visse ukjente, skadelige eller mistenkelige programmer og hva de gjør på enheten din. Denne informasjonen er anonym og sendes til F-Secure Corporation for kombinert dataanalyse. Vi bruker den analyserte informasjonen til å forbedre sikkerheten på din enhet og gi vern mot nye trusler og skadelige filer.

Hvordan sanntidsbeskyttelsesnettverket virker

Som bidragsyter til sanntidsbeskyttelsesnettverket kan du gi informasjon om ukjente programmer og nettsteder og om skadelige programmer og utnyttere på nettsteder. Sanntidsbeskyttelsesnettverket sporer ikke nettaktiviteten, samler ikke inn informasjon om nettsteder som allerede er analysert, og samler heller ikke inn informasjon om rene programmer som er installert på datamaskinen din.

Hvis du ikke ønsker å bidra, vil ikke sanntidsbeskyttelsesnettverket samle inn informasjon om installerte programmer eller besøkte nettsteder. Produktet må imidlertid sende en forespørsel til F-Secure-servere om ryktet til programmer, nettsteder, meldinger og andre objekter. Spørringen gjøres med en kryptografisk sjekksum der selve objektet det spørres om, ikke blir sendt til F-Secure. Vi sporer ikke data per bruker. Det er bare trefftelleren til filen eller nettstedet som økes.

Det er ikke mulig å stanse all nettverkstrafikk til sanntidsbeskyttelsesnettverket fullstendig fordi det er en integrert del av beskyttelsen som produktet gir.

Fordeler ved sanntidsbeskyttelsesnettverket

Med sanntidsbeskyttelsesnettverket vil du få raskere og mer nøyaktig beskyttelse mot de nyeste truslene, og du vil ikke motta unødvendige varsler om mistenkelige programmer som ikke er skadelige.

Som bidragsyter til sanntidsbeskyttelsesnettverket kan du hjelpe oss med å finne nye og hittil ukjente skadeprogrammer og fjerne "falske positiver" fra databasen med virusinfeksjoner.

Alle deltakere i sanntidsbeskyttelsesnettverket hjelper hverandre. Når sanntidsbeskyttelsesnettverket finner et mistenkelig program på enheten din, kan du dra nytte av analyseresultatene hvis samme program allerede er funnet på andre enheter. Sanntidsbeskyttelsesnettverket forbedrer den generelle ytelsen på enheten din fordi det installerte sikkerhetsproduktet ikke trenger å skanne programmer som sanntidsbeskyttelsesprogrammet har analysert og funnet rene. Og informasjon om skadelige nettsteder og uoppfordrede masseutsendelser deles gjennom sanntidsbeskyttelsesnettverket slik at vi kan gi deg mer nøyaktig beskyttelse mot nettstedsutnyttere og søppelmeldinger.

Jo flere som bidrar til sanntidsbeskyttelsesnettverket, dess bedre blir de enkelte deltakerne beskyttet.

Hvilke data du bidrar med

Som en bidragsyter til sanntidsbeskyttelsesnettverket bidrar du med informasjon om programmer som er lagret på din enhet og på nettstedene du besøker, slik at sanntidsbeskyttelsesnettverket kan gi beskyttelse mot de nyeste skadelige programmene og mistenkelige nettstedene.

Analysere filryktet

Sanntidsbeskyttelsesnettverket samler bare inn informasjon om programmer som ikke har et kjent rykte, og om filer som er mistenkelige eller kjent for å være skadelige.

Sanntidsbeskyttelsesnettverket samler in anonym informasjon om rene og mistenkelige programmer på enheten din. Sanntidsbeskyttelsesnettverket samler bare inn informasjon om utførbare filer (som filer med filtypene .cpl, .exe, .dll, .ocx, .sys, .scr og .drv på Windows-plattformen).

Innsamlet informasjon omfatter:

- filbanen til der programmet er på enheten din,
- størrelsen på filen og når den ble opprettet eller endret,
- filattributter og rettigheter,
- informasjon om filsignatur,
- gjeldende versjon av filen og firmaet som opprettet den,
- filopphavet og nedlastings-URL og
- F-Secure DeepGuard og antivirus-analyseresultater fra skannede filer og
- annen liknende informasjon.

Sanntidsbeskyttelsesnettverket samler aldri inn informasjon om dine personlige dokumenter, med mindre de er blitt infisert. For alle typer skadelige filer blir navnet på infeksjonen og desinfeksjonsstatus for filen samlet inn.

Med Sanntidsbeskyttelsesnettverk kan du også sende mistenkelige programmer til analyse. Du kan bare sende flyttbare utførbare filer. Sanntidsbeskyttelsesnettverket vil aldri samle inn informasjon om dine personlige dokumenter, og de blir aldri automatisk lastet opp for analyse.

Sende filer til analyse

Med sanntidsbeskyttelsesnettverket kan du også sende inn mistenkelige programmer for analyse.

Du kan sende inn mistenkelige enkeltprogrammer manuelt når produktet viser en melding om det. Du kan bare sende inn portable utførbare filer. Sanntidsbeskyttelsesnettverket laster aldri opp personlige dokumenter.

Analysere ryktet til et nettsted

Sanntidsbeskyttelsesnettverket sporer ikke din Internett-aktivitet og samler ikke inn informasjon om nettsteder som allerede er analysert. Det sikrer at nettstedene du besøker, er sikre mens du bruker Internett. Når du besøker et nettsted, vil sanntidsbeskyttelsesnettverket sjekke sikkerheten og varsle deg hvis stedet er vurdert som mistenkelig eller skadelig.

Hvis nettstedet du besøker, inneholder skadelig eller mistenkelig innhold eller en kjent utnytter, vil sanntidsbeskyttelsesnettverket samle inn hele URLen til stedet slik at nettsideinnholdet kan bli analysert.

Hvis du besøker et nettsted som ennå ikke er vurdert, vil sanntidsbeskyttelsesnettverket samle inn navn på domene og underdomene, og i enkelte tilfeller banen til den besøkte siden, slik at stedet kan analyseres og vurderes. Alle URL-parameterne som sannsynligvis inneholder informasjon som kan kobles til deg i et personlig identifiserbart format, blir fjernet for å beskytte personvernet.

Merk: Sanntidsbeskyttelsesnettverket vil ikke vurdere eller analysere nettsider i private nettverk, så det blir aldri samlet inn informasjon om private IP-nettverksadresser (for eksempel intranett i bedrifter).

Analysere systeminformasjonen

Sanntidsbeskyttelsesnettverket vil samle inn navn og versjon for operativsystemet ditt, informasjon om Internett-tilkoblingen og bruksstatistikk for sanntidsbeskyttelsesnettverket (for eksempel antall ganger ryktet til et nettsted er blitt forespurt og gjennomsnittlig tid før spørringen returnerte et resultat) slik at vi kan overvåke og forbedre tjenesten.

Hvordan vi beskytter personvernet

Vi overfører informasjon på en sikker måte, og vi fjerner automatisk alle personopplysninger som dataene kan inneholde.

Sanntidsbeskyttelsesnettverket fjerner identifiserende data før sending til F-Secure, og all innsamlet informasjon krypteres under overføringen for å beskytte mot uautorisert tilgang. De innsamlede dataene blir ikke behandlet enkeltvis, men settes sammen med informasjon fra andre bidragsytere til sanntidsbeskyttelsesnettverket. Alle data analyseres statistisk og anonymt, noe som betyr at ingen data kan kobles til deg på noen måte.

Eventuell informasjon som kan identifisere deg personlig, tas ikke med i de innsamlede dataene. Sanntidsbeskyttelsesnettverket samler ikke inn private IP-adresser eller din private informasjon, som e-postadresser, brukernavn og passord. Selv om vi gjør det vi kan for å fjerne alle data som kan identifisere deg personlig, er det mulig at noen identifiserende data forblir i den innsamlede informasjonen. I slike tilfeller vil vi ikke forsøke å bruke slike utilsiktet innsamlede data til å identifisere deg.

Vi har strenge sikkerhetstiltak og fysisk, administrativ og teknisk beskyttelse for å sikre den innsamlede informasjonen når den overføres, lagres og behandles. Informasjonen lagres sikkert på servere som styres av oss innenfor våre kontorer eller kontorene til våre underleverandører, og det er bare autorisert personell som får tilgang til den innsamlede informasjonen.

F-Secure kan dele innsamlede data med sine datterselskaper, underleverandører, distributører og partnere, men alltid i et ikke-identifiserbart, anonymt format.

Bli en bidragsyter til sanntidsbeskyttelsesnettverket

Du hjelper oss med å forbedre sanntidsbeskyttelsesnettverket ved å bidra med informasjon om skadelige programmer og nettsteder.

Du kan velge å delta i sanntidsbeskyttelsesnettverket under installeringen. Med standard installeringsinnstillinger vil du bidra til sanntidsbeskyttelsesnettverket. Du kan endre denne innstillingen senere.

Følg disse instruksjonene for å endre innstillingene for sanntidsbeskyttelsesnettverket:

1. Høyreklikk på ikonet helt til høyre på startrampen.
   Det vises en popup-meny.
2. Velg **Åpne fellesinnstillinger**.
3. Velg **Annet** > **Personvern**.
4. Merk av i boksen for å bli bidragsyter til sanntidsbeskyttelsesnettverket.

Spørsmål om Sanntidsbeskyttelsesnettverk

Kontaktinformasjon for alle spørsmål om Sanntidsbeskyttelsesnettverk.

Hvis du har flere spørsmål om sanntidsbeskyttelsesnettverket, kan du kontakte:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

http://www.f-secure.com/en/web/home_global/support/contact

Den nyeste versjonen av denne policyen er alltid tilgjengelig på nettstedet vårt.

Hvordan vet jeg at abonnementet mitt er gyldig

Abonnementstype og -status vises på siden **Abonnementsstatus**.

Når abonnementet er i ferd med å utløpe, eller hvis abonnementet er utløpt, endres den generelle beskyttelsestatusen til programmet på det tilsvarende ikonet på startrampen.

Slik kontrollerer du om abonnementet er gyldig:

1. Høyreklikk på ikonet helt til høyre på startrampen.
   Det vises en popup-meny.
2. Velg **Vis mine abonnementer**.
3. Velg **Abonnementsstatus** for å vise informasjon om abonnementene på installerte programmer.
4. Velg**Installeringsstatus** for å se hvilke programmer som er tilgjengelig for installering.

Abonnementsstatus og utløpsdato vises også på programmets **Statistikk**-side. Hvis abonnementet er utløpt, må du fornye det for å fortsette å motta oppdateringer og bruke produktet.

Merk: Når abonnementet er utløpt, blinker produktstatusikonet i systemfeltet.

Handlingssenter

Handlingssenteret viser alle viktige varsler som krever oppmerksomhet fra deg.

Hvis abonnementet har utløpt eller er i ferd med å utløpe, vil handlingssenteret ditt varsle om dette. Bakgrunnsfargen og innholdet i handlingssentermeldingen avhenger av abonnementstype og status:

- Hvis abonnementet er i ferd med å utløpe, og det er gratisabonnementer tilgjengelig, har meldingen en hvit bakgrunn og en **Aktiver**-knapp.
- Hvis abonnementet er i ferd med å utløpe og det ikke er noen gratisabonnementer tilgjengelig, har meldingen en gul bakgrunn og knappene **Kjøp** og **Oppgi nøkkel**. Hvis du allerede har kjøpt et nytt abonnement, kan du klikke på **Oppgi nøkkel** for å oppgi abonnementsnøkkelen og aktivere det nye abonnementet.
- Hvis abonnementet er utløpt, og det er gratisabonnementer tilgjengelig, har meldingen en rød bakgrunn og en **Aktiver**-knapp.
- Hvis abonnementet er utløpt og det ikke er noen gratisabonnementer tilgjengelig, har meldingen en rød bakgrunn og knappene **Kjøp** og **Oppgi nøkkel**. Hvis du allerede har kjøpt et nytt abonnement, kan du klikke på **Oppgi nøkkel** for å oppgi abonnementsnøkkelen og aktivere det nye abonnementet.

Merk: Lenken **Vis varslingshistorikk** i handlingssenteret viser en liste over produktvarsler, ikke tidligere handlingssentermeldinger.

Aktivere et abonnement

Når du har en ny abonnementsnøkkel eller kampanjekode for et produkt, må du aktivere den.

Slik aktiverer du et abonnement:

1. Høyreklikk på ikonet helt til høyre på startrampen.
   Det vises en popup-meny.
2. Velg **Vis mine abonnementer**.

3. Velg ett av følgende:
   - Klikk på **Aktiver abonnement**.
   - Klikk på **Aktiver kampanjekode**.
4. I dialogboksen som åpnes, angir du din nye abonnementsnøkkel eller kampanjekode og klikker på **OK**.

   Tips: Hvis du mottok abonnementsnøkkelen via e-post, kan du kopiere nøkkelen fra e-postmeldingen og lime den inn i feltet.

Når du har skrevet inn den nye abonnementsnøkkelen, vises gyldighetsdatoen for abonnementsnøkkelen på **Abonnementsstatus**-siden.

Kapitel

3

Innledning

Emner:

- *Vis den generelle statusen for beskyttelsen*
- *Vise produktstatistikken*
- *Håndtere produktoppdateringene*
- *Hva er virus og annen skadelig programvare*

Dette produktet beskytter datamaskinen mot virus og andre skadelige programmer.

Produktet skanner filer, analyserer programmer og oppdateres automatisk. Det krever ingen inngripen fra deg.

Vis den generelle statusen for beskyttelsen

Status-siden viser en kort oversikt over installerte produktfunksjoner og gjeldende status for disse.

Slik åpner du **Status**-siden:

Klikk på **Status** på hovedsiden.

Status-siden åpnes.

Ikonene angir status for programmet og dets sikkerhetsfunksjoner.

Statusikon	Statusnavn	Beskrivelse
	OK	Datamaskinen er beskyttet. Funksjonen er slått på og virker som den skal.
	Informasjon	Produktet informerer deg om en spesiell status for en funksjon. For eksempel blir funksjonen oppdatert.
	Advarsel	Datamaskinen er ikke beskyttet fullt ut. Produktet har for eksempel ikke mottatt oppdateringer på en lang stund, eller statusen for en funksjon krever oppmerksomhet.
	Feil	Datamaskinen er ikke beskyttet For eksempel kan abonnementet ditt ha utløpt, eller en kritisk funksjon er slått av.
	Av	En ikke-kritisk funksjon er slått av.

Vise produktstatistikken

Du kan se hva produktet har gjort siden det ble installert, på **Statistikk**-siden.

Slik åpner du **Statistikk**-siden:

Klikk på **Statistikk** på hovedsiden.

Siden **Statistikk** åpnes.

- **Siste vellykkede oppdateringskontroll** viser tidspunktet for den siste oppdateringen.

- **Virus- og spionprogramskanning** viser hvor mange filer produktet har skannet og og renset siden produktet ble installert.
- **Programmer** viser hvor mange programmer DeepGuard har tillatt eller blokkert siden det ble installert.
- **Brannmurtilkoblinger** viser antall tillatte og blokkerte tilkoblinger siden installeringen.
- **Søppelpost- og phishing-filtrering** viser hvor mange e-postmeldinger produktet har identifisert som gyldige e-postmeldinger, og hvor mange som er identifisert som søppelpostmeldinger.

Håndtere produktoppdateringene

Produktet holder automatisk beskyttelsen oppdatert.

Vise databaseversjoner

Du kan se tidspunktene for de siste oppdateringene og versjonsnumrene på siden **Databaseoppdateringer**.

Slik åpner du siden **Databaseoppdateringer**:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Andre innstillinger** > **Databaseversjoner**.

Siden **Databaseversjoner** viser den siste datoen da virus- og spionprogramdefinisjonene, DeepGuard og søppelpost- og phishing-filtrering ble oppdatert, sammen med versjonsnumrene.

Endre innstillingene for mobilt bredbånd

Velg om du vil laste ned sikkerhetsoppdateringer når du bruker mobilt bredbånd.

Merk: Denne funksjonen er tilgjengelig bare i Microsoft Windows 7.

Sikkerhetsoppdateringer vil som standard alltid lastes ned når du er innenfor hjemmeoperatørens nettverk. Oppdateringene stanses imidlertid midlertidig når du besøker nettverket til en annen operatør. Det er fordi tilkoblingsprisene kan variere mellom operatører, for eksempel i ulike land. Du kan vurdere å beholde denne innstillingen uendret hvis du vil spare båndbredde og eventuelt kostnader under oppholdet.

Merk: Denne innstillingen gjelder bare for tilkoblinger med mobilt bredbånd. Når datamaskinen er koblet til et kablet eller trådløst nettver, blir produktet automatisk oppdatert.

Slik endrer du innstillingen:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Andre innstillinger** > **Mobilt bredbånd** > **Last ned sikkerhetsoppdateringer**.
3. Velg ønsket oppdateringalternativ for mobile tilkoblinger:
   - **Bare innenfor hjemmeoperatørens nettverk**

     Oppdateringer lastes alltid ned i hjemmeoperatørens nettverk. Når du besøker nettverket til en annen operatør, stanses oppdateringene midlertidig. Vi anbefaler at du velger dette alternativet for å holde sikkerhetsproduktet oppdatert til forventede kostnader.
   - **Aldri**

     Oppdateringer lastes ikke ned når du bruker mobilt bredbånd.
   - **Alltid**

Oppdateringer lastes alltid ned, uansett hvilket nettverk du bruker. Velg dette alternativet hvis du vil være sikker på at datamaskinens sikkerhet alltid er oppdatert, uavhengig av kostnadene.

4. Hvis du vil avgjøre dette for hver gang du forlater hjemmeoperatørens nettverk, velger du **Spør hver gang jeg forlater hjemmeoperatørens nettverk**.

Sikkerhetsoppdateringer midlertidig stanset

Sikkerhetsoppdateringene kan stanses midlertidig når du bruker mobilt bredbånd utenfor hjemmeoperatørens nettverk.

I slike tilfeller kan du se varselet **Stanset midlertidig** nederst til høyre på skjermen. Oppdateringene stanses midlertidig fordi tilkoblingsprisene kan variere mellom operatører, for eksempel i forskjellige land. Du kan vurdere å beholde denne innstillingen uendret hvis du vil spare båndbredde og eventuelt kostnader under oppholdet. Hvis du imidlertid vil endre innstillingene, klikker du på **Endre**-lenken.

Merk:

Denne funksjonen er tilgjengelig bare i Microsoft Windows 7.

Hva er virus og annen skadelig programvare

Skadelig programvare er programmer som er spesielt utviklet for å skade datamaskinen din, bruke datamaskinen din til ulovlige formål uten at du vet det eller stjele informasjon fra datamaskinen din.

Skadelig programvare kan:

- ta kontroll over nettleseren din,
- omdirigere dine søkeforsøk,
- vise uønsket reklame,
- spore nettstedene du besøker,
- stjele personlig informasjon, for eksempel dine bankopplysninger,
- bruke datamaskinen din til å sende søppelpost, og
- bruke datamaskinen din til å angripe andre datamaskiner.

Skadelig programvare kan også gjøre datamaskinen treg og ustabil. Det kan være grunn til å tro at du har *skadelig programvare* på datamaskinen hvis den plutselig blir svært treg og krasjer ofte.

Virus

Et virus er vanligvis et program som kan legge til seg selv i filer og reprodusere seg selv fortløpende. Virus kan endre og erstatte innholdet i andre filer på en måte som kan skade datamaskinen.

Et *virus* er et program som vanligvis installeres på datamaskinen uten at du vet det. Når viruset er installert, prøver det å reprodusere seg selv. Viruset

- bruker noen av datamaskinens systemressurser
- kan endre eller skade filer på datamaskinen
- vil sannsynligvis prøve å bruke datamaskinen din til å infisere andre datamaskiner
- kan tillate at datamaskinen din brukes til ulovlige formål.

Spionprogrammer

Spionprogrammer er programmer som samler inn personopplysninger om deg.

Spionprogrammer kan samle inn personlig informasjon, inkludert

- Internett-steder du har besøkt,
- e-postadresser fra datamaskinen din,
- passord eller
- kredittkortnumre.

Spionprogrammer installerer seg nesten alltid selv uten at du har tillatt det. Spionprogrammer kan bli installert sammen med et nyttig program, eller ved at du narres til å klikke på et alternativ i et villedende popupvindu.

Rootkits

Rootkits er programmer som gjør annen *skadelig programvare* vanskelig å finne.

Rootkits skjuler filer og prosesser. Vanligvis gjør de dette for å skjule skadelig aktivitet på datamaskinen. Hvis en rootkit skjuler *skadelig programvare*, er det ikke lett å oppdage at datamaskinen har skadelig programvare.

Dette produktet har en rootkit-skanner som skanner spesielt etter rootkits, slik at *skadelig programvare* ikke så enkelt kan skjule seg.

Risikoprogrammer

Risikoprogrammer er ikke laget spesielt for å skade datamaskinen, men de kan skade datamaskinen hvis de misbrukes.

Risikoprogrammer er ikke strengt tatt skadelig programvare. Risikoprogrammer utfører enkelte nyttige, men potensielt farlige, funksjoner.

Eksempler på risikoprogrammer:

- programmer for direktemeldingstjenester, som IRC (Internet relay chat),
- programmer for filoverføring via Internett fra en datamaskin til en annen,
- eller Internett-telefonprogrammer (VoIP, *Voice Over Internet Protocol*).
- fjerntilgangsprogramvare, som VNC
- "skremmeprogrammer" som prøver å skremme eller svindle personer for å få dem til å kjøpe falsk sikkerhetsprogramvare
- programvare som er laget for å omgå CD-kontroller eller kopibeskyttelse.

Hvis du spesifikt har installert programmet og konfigurert det riktig, er det mindre sannsynlig at det er skadelig.

Hvis risikoprogrammet er installert uten at du visste det, er det sannsynligvis installert med ondsinnede hensikter og bør fjernes.

Kapitel

4

Beskytte datamaskinen mot skadelig programvare

Emner:

- *Hvordan skanne datamaskinen*
- *Hvordan ekskludere filer fra skanningen*
- *Hvordan bruke karantenen*
- *Hva er DeepGuard*
- *Hva er en brannmur*
- *Blokkere søppelpost*

Virus- og spionprogramskanning beskytter datamaskinen mot programmer som kan stjele personopplysninger, skade datamaskinen eller bruke den til ulovlige formål.

Som standard blir alle typer skadeprogrammer håndtert straks de blir funnet slik at de ikke forårsaker skade.

Som standard vil skanning etter virus og spionprogrammer automatisk skanne de lokale harddiskene, eventuelle flyttbare medier (som flyttbare stasjoner eller CDer) og nedlastet innhold. Du kan også angi at e-post skal skannes automatisk.

Skanning etter virus og spionprogrammer overvåker også datamaskinen for å oppdage eventuelle endringer som kan være tegn på *skadelig programvare*. Hvis det oppdages farlige systemendringer, for eksempel i systeminnstillinger eller forsøk på å endre viktige systemprosesser, hindrer DeepGuard at dette programmet kjøres, fordi det er sannsynlig at det kan være *skadelig programvare*.

Hvordan skanne datamaskinen

Når virus- og spionprogramskanning er slått på, skannes datamaskinen for skadelige filer automatisk. Du kan også skanne filer manuelt og planlegge skanninger.

Vi anbefaler at du alltid lar virus- og spionprogramskanning være slått på. Skann filene dine manuelt når du vil forsikre deg om at det ikke er noen skadelige filer på datamaskinen, eller hvis du vil skanne filer som du har ekskludert fra sanntidsskanningen.

Hvis du setter opp en planlagt skanning, vil virus- og spionprogramskanning fjerne skadelige filer fra datamaskinen på de angitte tidspunktene.

Skanne filer automatisk

Sanntidsskanning beskytter datamaskinen ved å skanne alle filer når de åpnes, og blokkere tilgang til filer som inneholder *skadelig programvare*.

Når datamaskinen forsøker å åpne en fil, vil sanntidsskanning skanne filen før datamaskinen får tilgang til den. Hvis sanntidsskanning finner noe skadelig innhold, setter den filen i karantene før den kan gjøre noe skade.

Vil sanntidsskanning påvirke ytelsen til datamaskinen?

Du legger normalt sett ikke merke til skanneprosessen fordi den bruker lite tid og systemressurser. Tiden og systemressursene som brukes i sanntidsskanningen, avhenger av for eksempel innholdet, plasseringen og typen fil.

Filer som det tar lenger tid å skanne:

- Filer på flyttbare stasjoner som CDer, DVDer og portable USB-stasjoner.
- Komprimerte filer, for eksempel *.zip*- filer.

  Merk: Komprimerte filer skannes ikke som standard.

Sanntidsskanning kan redusere datamaskinens hastighet hvis

- du har en datamaskin som ikke oppfyller systemkravene, eller
- du bruker mange filer samtidig. For eksempel når du åpner en katalog som inneholder mange filer som må skannes.

Slå sanntidsskanning på eller av

La sanntidsskanning være slått på for å stoppe *skadeprogrammer* før de kan skade datamaskinen.

Slik slår du sanntidsskanning på eller av:

1. Klikk på **Status** på hovedsiden.
2. Klikk på **Endre innstillinger på denne siden**.

   Merk: Du må ha administrative rettigheter for å slå av sikkerhetsfunksjoner.

3. Slå **Virus- og spionprogramskanning** på eller av.
4. Klikk på **Lukk**.

Håndtere skadelige filer automatisk

Sanntidsskanning kan håndtere skadelige filer automatisk uten å stille spørsmål til deg.

Slik lar du sanntidsskanning håndtere skadelige filer automatisk:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Datamaskinsikkerhet** > **Virus- og spionprogramskanning**.
3. Velg **Håndter skadelige filer automatisk**.

Hvis du velger ikke å håndtere skadelige filer automatisk, vil sanntidsskanning spørre deg hva du vil gjøre når en skadelig fil blir funnet.

Håndtere spionprogrammer

Virus- og spionprogramskanning blokkerer spionprogrammer umiddelbart når de forsøker å starte.

Før et spionprogram kan starte, vil produktet blokkere det og la deg avgjøre hva du vil gjøre med det.

Velg en av følgende handlinger når det blir oppdaget et spionprogram:

Handling som skal utføres	Hva skjer med spionprogrammet?
Håndter automatisk	La produktet avgjøre hva som er den beste handlingen, basert på spionprogrammet som ble funnet.
Sett spionprogrammet i karantene	Flytt spionprogrammet til karantenen der det ikke kan skade datamaskinen.
Slett spionprogrammet	Fjern alle spionprogramrelaterte filer fra datamaskinen.
Bare blokker spionprogrammet	Blokker tilgang til spionprogrammet, men la det være på datamaskinen.
Ekskluder spionprogrammet fra skanning	Tillat at spionprogrammet kjører, og ekskluder det fra fremtidige skanninger.

Håndtere risikoprogrammer

Virus- og spionprogramskanning blokkerer risikoprogrammer umiddelbart når de forsøker å starte.

Før et risikoprogram kan starte, vil produktet blokkere det og la deg avgjøre hva som skal gjøres med det.

Velg en av følgende handlinger når det blir oppdaget et risikoprogram:

Handling som skal utføres	Hva skjer med risikoprogrammet
Bare blokker riskoprogrammet	Blokker tilgang til risikoprogrammet, men la det være på datamaskinen.
Sett risikoprogrammet i karantene	Flytt risikoprogrammet til karantenen der det ikke kan skade datamaskinen.
Slett risikoprogrammet	Fjern alle risikoprogramrelaterte filer fra datamaskinen.
Ekskluder risikoprogrammet fra skanning	Tillat at risikoprogrammet kjører, og ekskluder det fra fremtidige skanninger.

Fjern sporings-informasjonskapsler automatisk

Ved å fjerne sporingskapsler hindres nettsteder i å spore hvilke områder du besøker på Internett.

Sporingskapsler er små filer som gjør det mulig for nettsteder å registrere hvilke netttsteder du besøker. Følg disse instruksjonene for å holde sporings-informasjonskapler unna datamaskinen.

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Datamaskinsikkerhet** > **Virus- og spionprogramskanning**.
3. Velg **Fjern sporings-informasjonskapsler**.
4. Klikk på **OK**.

Skanne filer manuelt

Du kan skanne filene dine manuelt, for eksempel når du kobler en ekstern enhet til datamaskinen, for å forsikre deg om at de ikke inneholder noen skadeprogrammer.

Starte den manuelle skanningen

Du kan skanne hele datamaskinen eller skanne etter en spesifikk type *skadelig programvare* eller en spesifikk plassering.

Hvis du har mistanke om en bestemt type *skadelig programvare*, kan du skanne etter bare denne typen. Hvis du har mistanke til en bestemt plassering på datamaskinen, kan du skanne bare denne plasseringen. Disse skanningene blir fullført mye raskere enn en skanning av hele datamaskinen.

Slik starter du manuell skanning av datamaskinen:

1. Klikk på pilen under **Skann** på hovedsiden.

   Skannealternativene vises.
2. Velg type skanning.

   Velg **Endre skanneinnstillinger** for å optimalisere måten den manuelle skanningen skanner datamaskinen for virus og andre skadelige programmer.
3. Hvis du valgte **Velg hva som skal skannes**, åpnes et vindu der du kan velge plasseringen som skal skannes.
   Skanneveiviser åpnes.

Typer skanninger

Du kan skanne hele datamaskinen eller skanne etter en spesifikk type skadelig programvare eller en spesifikk plassering.

Nedenfor ser du en liste over de forskjellige typene skanning:

Skannetype	Hva skannes	Når skal denne typen brukes
Virus- og spionprogramvern	Skanner deler av datamaskinen for virus, spionprogrammer og risikoprogrammer	Denne typen skanning er mye raskere enn en full skanning. Den søker bare i delene av systemet som inneholder installerte programfiler. Denne skannetypen anbefales hvis du raskt vil sjekke om datamaskinen er ren, fordi den på en effektiv måte finner og fjerner alle aktive skadeprogrammer på datamaskinen.
Full datamaskinskanning	Hele datamaskinen (interne og eksterne harddisker) skannes for virus, spionprogrammer og risikoprogrammer	Når du vil være helt sikker på at det ikke er skadelig programvare eller risikoprogrammer på datamaskinen. Denne typen skanning tar lengst tid. Den kombinerer rask skadeprogramskanning og harddiskskanning. Den ser også etter elementer som kan være skjult av en rootkit.
Velg hva som skal skannes	En spesifikk fil, mappe eller stasjon skannes for virus, spionprogrammer og risikoprogrammer	Hvis du mistenker at en bestemt plassering på datamaskinen kan ha skadelig programvare , for eksempel hvis plasseringen inneholder nedlastinger fra potensielt farlige kilder som fildelingsnettverk. Tiden skanningen vil ta, avhenger av størrelsen på

Skannetype	Hva skannes	Når skal denne typen brukes
		målet du skanner. Skanningen fullføres raskt hvis du for eksempel skanner en mappe som bare inneholder noen få små filer.
Rootkit-skanning	Skanner viktige plasseringer i systemet der et mistenkelig element kan medføre et sikkerhetsproblem. Søker etter skjulte filer, mapper, stasjoner eller prosesser	Når du mistenker at det kan være installert rootkit på datamaskinen. Hvis for eksempel skadelig programvare nylig ble oppdaget på datamaskinen, og du vil forsikre deg om at den ikke installerte et rootkit.

Skann i Windows Utforsker

Du kan skanne disker, mapper og filer for *virus*, *spionprogrammer* og *risikoprogrammer* i Windows Utforsker.

Slik skanner du en disk, mappe eller fil:

1. Plasser musepekeren på disken, mappen eller filen du vil skanne, og høyreklikk.
2. Velg **Skann mapper for virus** fra hurtigmenyen. (Navnet på alternativet avhenger av om du skanner en disk, mappe eller fil.)
   Vinduet **Skanneveiviser** åpnes, og skanningen starter.

Hvis det blir funnet *virus* eller *spionprogrammer*, vil **Skanneveiviser** lede deg gjennom renseprosessen.

Velge filer som skal skannes

Velg filtypene som du vil skal skannes for *virus* og *spionprogrammer* i manuelle og planlagte skanninger.

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Andre innstillinger** > **Manuell skanning**.
3. Under **Skannealternativer** velger du fra følgende innstillinger:

   Skann bare kjente filtyper — For å skanne bare de filtypene som mest sannsynlig blir infisert, for eksempel utførbare filer. Skanningen går også raskere hvis velger dette alternativet. Filer med følgende filtyper skannes: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` og `.hqx`.

   Skann i komprimerte filer — For å skanne arkivfiler og -mapper.

   Bruk avansert heuristikk — For å bruke all tilgjengelig heuristikk under skanningen for å forbedre søk etter ny eller ukjent skadelig programvare.

   Merk: Hvis du velger dette alternativet, tar skanningen lengre tid og kan resultere i flere falske funn (harmløse filer som rapporteres som mistenkelige).

4. Klikk på **OK**.

Merk: Ekskluderte filer i listen over ekskluderte elementer, blir ikke skannet selv om du velger dem for skanning her.

Hva du bør gjøre når det oppdages skadelige filer

Velg hvordan du vil håndtere skadelige filer når de blir funnet.

Slik velger du handling som skal utføres når det blir funnet skadelig innhold under den manuelle skanningen:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Andre innstillinger** > **Manuell skanning**.
3. Velg fra følgende alternativer i **Når virus eller spionprogrammer blir funnet**:

Alternativ	Beskrivelse
Spør meg (standard)	Du kan velge handlingen som skal utføres for hvert element som blir funnet under manuell skanning.
Rense filene	Produktet prøver automatisk å desinfisere infiserte filer som blir funnet under manuell skanning. **Merk:** Hvis produktet ikke kan rense den infiserte filen, settes den i karantene (unntatt hvis den blir funnet på nettverks- eller flyttbare stasjoner) slik at den ikke kan skade datamaskinen.
Sett filene i karantene	Produktet flytter alle skadelige filer som blir funnet under en manuell skanning, til karantenen, der de ikke kan skade datamaskinen.
Slett filene	Produktet sletter alle skadelige filer som blir funnet under en manuell skanning.
Bare rapporter	Produktet lar alle skadelige filer som ble funnet under en manuell skanning, være som de er, og registrerer den funnet i skannerapporten. **Merk:** Hvis sanntidsskanning ikke er slått på, vil skadelig programvare kunne skade datamaskinen hvis du velger dette alternativet.

Merk: Når det blir funnet skadelige filer under planlagt skanning, renses de automatisk.

Planlegge en skanning

Angi at datamaskinen skal skanne og fjerne virus og andre skadelige programmer automatisk når du ikke bruker den, eller angi at skanning skal kjøres med jevne mellomrom for å forsikre deg om at datamaskinen er ren.

Slik planlegger du en skanning:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Andre innstillinger** > **Planlagt skanning**.
3. Slå på **Planlagt skanning**.
4. Velg når skanningen skal starte.

Alternativ	Beskrivelse
Daglig	Skann datamaskinen hver dag.
Ukentlig	Skann datamaskinen på valgte ukedager. Velg dagene fra listen.

Alternativ	Beskrivelse
Månedlig	Skann datamaskinen på valgte dager i måneden. Slik velger du dager: 1. Velg et av alternativene for Dag. 2. Velg dagen i måneden fra listen ved siden av den valgte dagen.

5. Velg når du vil starte skanningen på de valgte dagene.

Alternativ	Beskrivelse
Starttidspunkt	Start skanningen på angitt tidspunkt.
Når maskinen ikke har vært i bruk i	Start skanningen når datamaskinen ikke har vært brukt i løpet av en angitt tidsperiode.

Planlagt skanning bruker innstillingene for manuell skanning når datamaskinen skannes, bortsett fra at den skanner arkiver hver gang og renser skadelige filer automatisk.

Skanne e-postmeldinger

E-postskanning beskytter deg mot skadelige filer i e-postmeldinger som sendes til deg.

Virus- og spionprogramskanning må være slått på for å skanne e-postmeldinger for virus.

Slik slår du på skanning av e-post:

1. Klikk på Innstillinger på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg Datamaskinsikkerhet > Virus- og spionprogramskanning.
3. Velg Fjern skadelige e-postvedlegg.
4. Klikk på OK.

Når blir e-postmeldinger og vedlegg skannet

Virus- og spionprogramskanning kan fjerne skadelig innhold fra e-post som du mottar.

Virus- og spionprogramskanning fjerner skadelige e-postmeldinger som mottas av e-postprogrammer som Microsoft Outlook og Outlook Express, Microsoft Mail eller Mozilla Thunderbird. Det skanner ukrypterte e-postmeldinger og vedlegg hver gang e-postprogrammet mottar dem fra postserveren med POP3-protokoll.

Virus- og spionprogramskanning kan ikke skanne e-postmeldinger i webmail, som inkluderer e-postprogrammer som kjører i nettlesere, som Hotmail, Yahoo! mail eller Gmail. Du er fremdeles beskyttet mot *virus* selv om du ikke fjerner skadelige vedlegg eller bruker webmail. Når du åpner e-postvedlegg, vil sanntidsskanning fjerne alle skadelige vedlegg før de kan gjøre noe skade.

Merk: Sanntidsskanning beskytter bare datamaskinen, ikke vennene dine. Sanntidsskanning kan ikke skanne vedlagte filer hvis du ikke åpner vedlegget. Dette betyr at hvis du bruker webmail og videresender en melding før du åpner vedlegget, kan du videresende en infisert e-postmelding til vennene dine.

Vise skanneresultatene

Virus- og spionprogramhistorikk viser alle skadelige filer som produktet har funnet.

Enkelte ganger kan ikke produktet utføre handlingen du har valgt, når noe skadelig blir funnet. For eksempel, hvis du velger å rense filer og en fil ikke kan renses, flytter produktet filen til karantenen. Du kan vise denne informasjonen i virus- og spionprogramhistorikken.

Slik viser du historikken:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Datamaskinsikkerhet** > **Virus- og spionprogramskanning**.
3. Klikk på **Vis fjerningshistorikk**.

Virus- og spionprogramhistorikken viser følgende informasjon:

- Datoen og klokkeslettet da den skadelige filen ble funnet,
- navnet på skadeprogrammet og plasseringen på datamaskinen, og
- handlingen som ble utført.

Hvordan ekskludere filer fra skanningen

Noen ganger ønsker du kanskje å ekskludere enkelte filer eller programmer fra skanningen. Ekskluderte elementer skannes ikke hvis du ikke fjerner dem fra listen over ekskluderte elementer.

Merk: Det er separate eksklusjonslister for sanntidsskanning og manuell skanning. Hvis du for eksempel ekskluderer en fil fra sanntidsskanning, skannes den under manuell skanning hvis du ikke også ekskluderer den fra manuell skanning.

Ekskludere filtyper

Når du ekskluderer filer etter type, blir ikke filer med de angitte filtypene skannet for skadelig innhold.

Slik legger du til eller fjerner filtyper som du vil ekskludere:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg om du vil ekskludere filtypen fra sanntidsskanning eller manuell skanning:
   - Velg **Datamaskinsikkerhet** > **Virus- og spionprogramskanning** for å ekskludere filtypen fra sanntidsskanning.
   - Velg **Andre innstillinger** > **Manuell skanning** for å ekskludere filtypen fra manuell skanning.
3. Klikk på **Ekskluder filer fra skanningen**.
4. Slik ekskluderer du en filtype:
   a) Velg kategorien **Filtyper**.
   b) Velg **Ekskluder disse filtypene**.
   c) Skriv en filtype som identifiserer typen filer du vil ekskludere, i feltet ved siden av knappen **Legg til**.

      Hvis du vil angi filer som ikke har noen filtype, skriver du ".". Du kan bruke jokertegnet "?" for å representere ett enkelt tegn, eller "*" for å representere hvilket som helst antall tegn.

      Hvis du for eksempel vil ekskludere utførbare filer, skriver du `exe` i feltet.
   d) Klikk på **Legg til**.
5. Gjenta forrige trinn for alle andre filtyper du vil ekskludere fra skanning etter virus.
6. Klikk på **OK** for å lukke dialogboksen **Ekskluder fra skanning**.
7. Klikk på **OK** for å bruke de nye innstillingene.

De valgte filtypene blir ekskludert fra fremtidige skanninger.

Ekskludere filer etter plassering

Når du ekskluderer filer etter plassering, blir ikke filer på angitte stasjoner eller i angitte mapper skannet for skadelig innhold.

Slik legger du til eller fjerner filplasseringer som du vil ekskludere:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg om du vil ekskludere plasseringen fra sanntidsskanning eller manuell skanning:
   - Velg **Datamaskin** > **Virus- og spionprogramskanning** for å ekskludere plasseringen fra sanntidsskanning.
   - Velg **Datamaskin** > **Manuell skanning** for å ekskludere plasseringen fra manuell skanning.
3. Klikk på **Ekskluder filer fra skanningen**.
4. Slik ekskluderer du en fil, mappe eller stasjon:
   a) Velg kategorien **Objekter**.
   b) Velg **Ekskluder objekter (filer, mapper, ...)**.
   c) Klikk på **Legg til**.
   d) Velg filen, stasjonen eller mappen du vil ekskludere fra virusskanning.

      Merk: Enkelte stasjoner kan være flyttbare, som CD-, DVD- eller nettverksstasjoner. Nettverksstasjoner og tomme flyttbare stasjoner kan ikke ekskluderes.

   e) Klikk på **OK**.
5. Gjenta forrige trinn for å ekskludere andre filer, stasjoner eller mapper fra virusskanninger.
6. Klikk på **OK** for å lukke dialogboksen **Ekskluder fra skanning**.
7. Klikk på **OK** for å aktivere de nye innstillingene.

De valgte filene, stasjonene eller mappene blir ekskludert fra fremtidige skanninger.

Vise ekskluderte programmer

Du kan vise programmer du har ekskludert fra skanning, og fjerne dem fra listen over ekskluderte elementer hvis du i fremtiden vil skanne dem.

Hvis sanntidsskanning eller manuell skanning oppdager et program som oppfører seg som et spion- eller risikoprogram, men du vet at det er trygt, kan du ekskludere fra skanningen slik at produktet ikke varsler deg om det.

Merk: Hvis programmet oppfører seg som et virus eller annet skadeprogram, kan det ikke ekskluderes.

Du kan ikke ekskludere programmer direkte. Nye programmer vises på eksklusjonslisten bare hvis du ekskluderer dem under skanning.

Slik viser du programmene som er ekskludert fra skanning:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg om du vil vise programmer som har blitt ekskludert fra sanntidsskanning eller manuell skanning:
   - Velg **Datamaskin** > **Virus- og spionprogramskanning** for å vise programmer som er ekskludert fra sanntidsskanning.
   - Velg **Datamaskin** > **Manuell skanning** for å vise programmer som er ekskludert fra manuell skanning.

3. Klikk på **Ekskluder filer fra skanningen**.
4. Velg kategorien **Programmer**.

   Merk: Det er bare spion- og risikoprogrammer som kan ekskluderes, ikke virus.

5. Hvis du vil skanne det ekskluderte programmet igjen:
   a) Velg programmet du vil inkludere i skanningen.
   b) Klikk på **Fjern**.
6. Klikk på **OK** for å lukke dialogboksen **Ekskluder fra skanning**.
7. Klikk på **OK** for å avslutte.

Hvordan bruke karantenen

Karantenen er et sikkert lager for filer som kan være skadelige.

Filer som er i karantene, kan ikke spre seg eller skade datamaskinen.

Du kan plassere *skadelig programvare*, *spionprogrammer* og *risikoprogrammer* i karantene for å uskadeliggjøre dem. Du kan gjenopprette programmer eller filer fra karantenen senere, hvis du trenger dem.

Hvis du ikke trenger et element som er i karantene, kan du slette det. Når du sletter et element som ligger i karantene, blir det fjernet permanent fra datamaskinen.

- Vanligvis kan du slette *skadelig programvare* som ligger i karantene.
- I de fleste tilfeller kan du slette *spionprogrammer* som er i karantene. Det kan hende *spionprogrammene* i karantene tilhører legitim programvare, og hvis du fjerner dem, slutter selve programmet å fungere riktig. Hvis du vil beholde programmet på datamaskinen, kan du gjenopprette *spionprogrammene* i karantene.
- Et *risikoprogram* i karantene kan være legitim programvare. Hvis du har installert og konfigurert programmet selv, kan du gjenopprette det fra karantenen. Hvis *risikoprogrammet* er installert uten at du kjente til det, er det sannsynligvis installert med ondsinnede hensikter og bør slettes.

Vise elementer i karantene

Du kan vise mer informasjon om elementer i karantene.

Slik viser du detaljert informasjon om elementer i karantene:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Datamaskinsikkerhet** > **Virus- og spionprogramskanning**.
3. Klikk på **Vis karantene**.
   Karantene-siden viser totalt antall elementer som er lagret i karantenen.
4. Hvis du vil vise detaljert informasjon om elementer i karantene, klikker du på **Detaljer**.

   Du kan sortere innholdet etter skadelig programvare eller filbane.

   En liste over de 100 første elementene vises med type element i karantene, navnet på elementet og banen til plasseringen der filene ble installert.
5. Hvis du vil vise mer informasjon om et element i karantene, klikker du på -ikonet ved siden av elementet i **Tilstand**-kolonnen.

Gjenopprette elementer i karantene

Du kan gjenopprette elementer du trenger fra karantene.

Du kan gjenopprette programmer eller filer fra karantene hvis du trenger dem. Ikke gjenopprett elementer fra karantene med mindre du er sikker på at elementene ikke utgjør noen trussel. Gjenopprettede elementer flyttes tilbake til den opprinnelige plasseringen på datamaskinen.

Gjenopprette elementer i karantene

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Datamaskinsikkerhet** > **Virus- og spionprogramskanning**.
3. Klikk på **Vis karantene**.
4. Merk elementene du vil gjenopprette fra karantene.
5. Klikk på **Gjenopprett**.

Hva er DeepGuard

DeepGuard analyserer innholdet i filer og virkemåten til programmer, og overvåker programmer som ikke er klarerte.

DeepGuard blokkerer nye og uoppdagede *virus*, *ormer* og andre skadeprogrammer som prøver å gjøre endringer på datamaskinen din, og hindrer at mistenkelige programmer får tilgang til Internett.

Når DeepGuard oppdager et nytt program som prøver å foreta potensielt skadelige endringer i systemet, tillates programmet å kjøre i en sikker sone. I den sikre sonen kan ikke programmet skade datamaskinen. DeepGuard analyserer endringene som programmet forsøkte å gjøre, og basert på dette avgjøres det hvor sannsynlig det er at programmet er et *skadeprogram*. Hvis det er sannsynlig at programmet er et *skadeprogram*, vil DeepGuard blokkere det.

Potensielt skadelige systemendringer som DeepGuard oppdager, inkluderer:

- endringer i systeminnstillinger (Windows-registeret),
- forsøk på å slå av viktige systemprogrammer, for eksempel sikkerhetsprogrammer som dette produktet, og
- forsøk på å redigere viktige systemfiler.

Slå DeepGuard på eller av

La DeepGuard være slått på for å hindre at mistenkelige programmer gjør potensielt skadelige endringer på datamaskinen.

Hvis du har Windows XP, må du kontrollere at du har Service Pack 2 installert før du slår på DeepGuard.

Slik slår du DeepGuard på eller av:

1. Klikk på **Status** på hovedsiden.
2. Klikk på **Endre innstillinger på denne siden**.

   Merk: Du må ha administrative rettigheter for å slå av sikkerhetsfunksjoner.

3. Slå **DeepGuard** på eller av.
4. Klikk på **Lukk**.

Tillat programmer som DeepGuard har blokkert

Du kan styre hvilke programmer DeepGuard tillater og blokkerer.

Noen ganger kan DeepGuard blokkere et trygt program, selv om du vil bruke programmet og du vet at det er sikkert. Dette skjer fordi programmet prøver å gjøre systemendringer som kan være skadelige. Du kan også ha blokkert programmet ved en feiltagelse når en DeepGuard-melding har blitt vist.

Slik tillater du et program som DeepGuard har blokkert:

1. Klikk på **Verktøy** på hovedsiden.
2. Klikk på **Programmer**.
   Listen **Overvåkede programmer** vises.
3. Finn programmet du vil tillate.

   Merk: Du kan klikke på kolonneoverskrifter for å sortere listen. Du kan for eksempel klikke på **Tillatelse**-kolonnen for å sortere listen i grupper med tillatte og forbudte programmer.

4. Velg **Tillat** i **Tillatelse**-kolonnen.
5. Klikk på **Lukk**.

DeepGuard tillater at programmet gjør systemendringer igjen.

Bruke DeepGuard i kompatibilitetsmodus

For å gi maksimal beskyttelse endrer DeepGuard midlertidig programmer som kjører. Noen programmer kontrollerer at de ikke er skadet eller endret, og er kanskje ikke kompatible med denne funksjonen. For eksempel vil online-spill med verktøy som skal hindre juks, kontrollere at de ikke har blitt endret på noen måte når de kjøres. I slike tilfeller kan du slå på kompatibilitetsmodus.

Slik slår du på kompatibilitetsmodus:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Datamaskinsikkerhet** > **DeepGuard**.
3. Velg **Bruk kompatibilitetsmodus**.
4. Klikk på **OK**.

Hva du bør gjøre med varsler om mistenkelig virkemåte

DeepGuard overvåker programmer som ikke er klarerte. Hvis et overvåket program forsøker å bruke Internett, forsøker å endre systemet eller oppfører seg mistenkelig, vil DeepGuard blokkere det.

Når du har valgt **Varsle meg om mistenkelig virkemåte** i DeepGuard-innstillingene, vil DeepGuard varsle deg når det oppdager et potensielt skadelig program eller når du starter et program som ikke har et kjent omdømme.

Slik avgjør du hva du vil gjøre med programmet som DeepGuard har blokkert:

1. Klikk på **Detaljer** for å vise mer informasjon om programmet.
   Avsnittet med detaljer viser:
   - plasseringen til programmet,
   - omdømmet til programmet i sanntidsbeskyttelsesnettverket, og
   - hvor vanlig programmet er.
2. Avgjør om du stoler på programmet som DeepGuard har blokkert:
   - Velg **Jeg stoler på programmet. La det fortsette.** hvis du ikke vil blokkere programmet.

     Programmet er sannsynligvis sikkert hvis:

- DeepGuard blokkerte programmet på grunn av noe du gjorde,
- du kjenner igjen programmet, eller
- du har fått programmet fra en klarert kilde.

- Velg **Jeg stoler ikke på programmet. Blokker det.** hvis du vil at programmet fortsatt skal være blokkert.

  Programmet er sannsynligvis usikkert hvis:

  - programmet er uvanlig,
  - programmet har et ukjent omdømme, eller
  - du ikke kjenner programmet.

3. Hvis du vil sende et mistenkelig program til analyse:
   a) Klikk på **Rapporter programmet til F-Secure**.
   Produktet viser vilkårene for innsending.
   b) Klikk på **Godta** hvis du godtar vilkårene ig vil sende inn eksempelet.

   Vi anbefaler at du sender et eksempel når:

   - DeepGuard blokkerer et program du vet er sikkert, eller
   - du mistenker at programmet er et *skadeprogram*.

Hva er en brannmur

Brannmuren hindrer at inntrengere og skadelige programmer kommer inn på datamaskinen din fra Internett.

Brannmuren tillater bare sikre Internett-tilkoblinger fra datamaskinen din, og blokkerer inntrengere fra Internett.

Slå brannmuren på eller av

La brannmuren være slått på for å hindre at inntrengere får tilgang til datamaskinen din.

Slik slår du brannmuren på eller av:

1. Klikk på **Status** på hovedsiden.
2. Klikk på **Endre innstillinger på denne siden**.

   Merk: Du må ha administrative rettigheter for å slå av sikkerhetsfunksjoner.

3. Sett **Brannmur** til på eller av.

   Merk: Datamaskinen er ikke fullt beskyttet når du slår av sikkerhetsfunksjoner.

4. Klikk på **Lukk**.

Vi anbefaler at du ikke lar *brannmuren* være avslått. Hvis du gjør det, blir datamaskinen sårbar for alle nettverksangrep. Hvis et program slutter å virke fordi det ikke kan koble til Internett, endrer du *brannmurinnstillingene* i stedet for å slå av *brannmuren*.

Endre brannmurinnstillinger

Når brannmuren er slått på, begrenser den tilgang til og fra datamaskinen. Noen programmer kan kreve at du tillater tilgang gjennom brannmuren for at de skal virke riktig.

Produktet bruker Windows-brannmuren til å beskytte datamaskinen.

Slik endrer du innstillinger for Windows-brannmur:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Datamaskinsikkerhet** > **Brannmur**.
3. Klikk på **Endre innstillinger for Windows-brannmur**.

   Merk: Du må ha administrative rettigheter for å kunne redigere innstillingene.

Hvis du ønsker mer informasjon om Windows-brannmur, kan du se dokumentasjonen til Microsoft Windows.

Hindre programmer i å laste ned skadelige filer

Du kan hindre at programmer på datamaskinen laster ned skadelige filer fra Internett.

Noen nettsteder inneholder utnyttere og andre skadelige filer som kan skade datamaskinen. Med avansert nettverksbeskyttelse kan du hindre at programmer laster ned skadelige filer før de når datamaskinen din.

Slik blokkerer du et program fra å laste ned skadelige filer:

1. Klikk på **Innstillinger** på hovedsiden.

   Merk: Du må ha administrative rettigheter for å kunne endre innstillingene.

2. Velg **Datamaskinsikkerhet** > **Brannmur**.
3. Velg **Ikke tillat at programmer laster ned skadelige filer**.

Merk: Denne innstillingen vil være aktiv selv om du slår av brannmuren.

Blokkere søppelpost

Søppelpost- og phishing-filtrering beskytter datamaskinen mot *søppelpost*- og *phishing*-e-postmeldinger.

En e-postmelding anses som *søppelpost* hvis den sendes som en del av en større samling meldinger der alle har omtrent identisk innhold, og hvis mottakerne ikke har gitt verifiserbar tillatelse til at meldingen kan sendes. *Søppelpost*- og *phishing*-meldinger oversvømmer ofte ønskede e-postmeldinger.

Bruk søppelpost- og phishing-filtrering til å fange opp søppelpost- og phishing-meldinger og flytte dem til *søppelpost*-mappen.

Slå søppelpost- og phishing-filtrering på eller av

La søppelpost- og phishing-filtrering være slått på for å fjerne søppelpost- og phishing-meldinger fra innkurven.

Slik slår du søppelpost- og phishing-filtrering på eller av:

1. Klikk på **Status** på hovedsiden.
2. Klikk på **Endre innstillinger på denne siden**.

   Merk: Du må ha administrative rettigheter for å slå av sikkerhetsfunksjoner.

3. Slå **Søppelpost- og phishing-filtrering** på eller av.
4. Klikk på **Lukk**.

Beskytte mot phishing-forsøk

Søppelpost- og phishing-filtrering beskytter datamaskinen mot *phishing*-forsøk som bruker falske e-postadresser, og som virker å komme fra legitime bedrifter, for å stjele personlig informasjon.

Disse meldingene, som ser autentiske ut, er laget for å lure deg til å oppgi personlige data, som bankkontonumre, passord og kredittkort- og personnumre. Ikke stol på noen e-postmeldinger som oppdages av søppelpost- og phishing-filtrering.

Hvis du får en ny e-postmelding som identifiseres som et forsøk på *phishing*, blir den automatisk flyttet til *søppelpost*-mappen.

I Microsoft Outlook, Outlook Express og Windows Mail opprettes *phishing*-reglene automatisk. Hvis du bruker et annet e-postprogram, må du opprette filtreringsregler manuelt.

Konfigurere e-postprogrammet til å filtrere vekk søppelpost

Du kan opprette en *søppelpost*- og *phishing*-mappe og filtreringsregler i e-postprogrammet ditt for å filtrere vekk *søppelpost*.

E-postfiltrering oppretter en *søppelpost*- og en *phishing*-mappe og filtreringsregler automatisk i Microsoft Outlook, Microsoft Outlook Express og Windows Mail (i Windows Vista). Hvis du bruker et annet e-postprogram, må du opprette mappene og filtreringsreglene manuelt. Hvis du har flere e-postkonti, må du opprette filtreringsregler for hver e-postkonto separat.

Merk: *Søppelpost*- og *phishing*- filtrering støtter bare POP3-protokollen. Web-baserte e-postprogrammer eller andre protokoller støttes ikke.

Hvordan virker mine egne og e-postfiltreringsreglene sammen?	E-postfiltrering filtrerer e-postmeldinger basert på sine egne filtreringsregler. Programmet filtrerer ikke e-postmeldinger som stemmer med regler som du har laget. Hvis du for eksempel har opprettet en regel som filtrerer vekk alle e-postmeldinger fra en webbutikk til Webbutikk-mappen, blir både dine bestillingsbekreftelsesmeldinger og reklame fra den webbutikken flyttet ut av innkurven og filtrert til Webbutikk-mappen.

Dette avsnittet inneholder instruksjoner om hvordan du kan opprette en søppelpostmappe og filtreringsregler for e-postprogrammer fra Microsoft, Netscape, Mozilla Thunderbird og Eudora. Du kan også bruke disse instruksjonene til å opprette lignende filtreringsregler i andre e-postprogrammer.

E-postprogrammer fra Microsoft

E-postfiltrering oppretter automatisk mapper for *søppelpost* og *phishing*-meldinger og filtreringsregler i Microsoft Outlook, Microsoft Outlook Express og Windows Mail.

Merk: Automatisk filtrering virker kanskje ikke med e-postkontoer som er opprettet med Post-programmet i Windows Kontrollpanel. Hvis du mottar søppel- og phishing-meldinger etter at du har slått på e-postfiltrering, bruker du meldingsemnet `[SPAM]` til å filtrere søppelpost- og phishing-meldinger.

Blokkere søppelpost i Mozilla Thunderbird og Eudora OSE

Search title: Opprette filtreringsregel for søppelpost i Mozilla Thunderbird og Eudora OSE.

Når du skal filtrere *søppelpost*- og phishing-meldinger, må du opprette en søppelpostmappe og filtreringsregelen.

Slik oppretter du *søppelpost* -filtreringsregel:

1. Høyreklikk på **Lokale mapper**, og velg **Ny mappe**.
2. Angi `Søppelpost` som navn på den nye mappen.
3. Velg **Verktøy** > **Meldingsfiltre**.
4. Klikk på **Ny**.

5. Skriv `søppelpost` som **Filternavn**.
6. Opprett en matchende regel for å finne søppelpostmeldinger:
   a) Kontroller at **Emne** og **inneholder** er valgt i filtreringsvalgene.
   b) Skriv `[SPAM]` i det tredje feltet.
7. Opprett en handling som flytter søppelposten til søppelpostmappen:
   a) Velg **Flytt melding til** fra den første listen.
   b) Velg *søppelpost*-mappen i den andre nedtrekkslisten.
8. Klikk på **OK** for å lagre endringene.
9. Lukk dialogboksen **Meldingsfiltre**.

Du har nå opprettet filtreringsregelen for *søppelpost*. Heretter blir *søppelpost*meldinger filtrert til mappen *søppelpost*.

Blokkere søppelpost i Opera

Search title: Opprette regel for filtrering av søppelpost i Opera

Når du skal filtrere *søppelpost*- og phishing-meldinger, må du opprette en søppelpostmappe og filtreringsregelen.

Merk: Fremgangsmåten som er vist her, gjelder Opera versjon 11. Fremgangsmåten for andre versjoner kan variere litt.

Slik oppretter du en filtreringsregel for *søppelpost*:

1. Åpne visningen **Opera Mail**.
2. Høyreklikk på standard *Søppelpost*-mappe og velg **Egenskaper**.
3. Klikk på **Legg til regel**.
4. Opprett en regel for flytting av en e-postmelding til *søppelpost*mappen:
   a) Kontroller at **Emne** og **inneholder** er valgt i filtreringsvalgene.
   b) Skriv `[SPAM]` i det tredje feltet.
5. Klikk på **Lukk** for å bekrefte den nye *søppelpost*-filtreringsregelen.

Du har nå opprettet filtreringsregelen for *søppelpost*. Heretter blir *søppelpost*meldinger filtrert til mappen *søppelpost*.

Kapitel

5

Sikker bruk av Internett

Emner:

- *Hvordan kjøre vanlige oppgaver*
- *Slik beskytter du forskjellige brukerkontoer*
- *Hva er nettleserbeskyttelse*
- *Gjøre nettbruk sikker*
- *Hvordan angi surfetid*
- *Vise statistikk*

Informasjon om hvordan du kommer i gang med å bruke produktet.

Dette produktet hjelper deg og din familie med å bruke Internett trygt. I tillegg til å beskytte mot skadeprogrammer og skadelige nettsteder, kan du også begrense typen innhold som kan vises av de forskjellige brukerkontoene.

Produktet bruker Windows-brukerkontoer til å styre innstillingene for hver person som bruker datamaskinen. Det er bare brukere med administrative tilgangsrettigheter som kan endre produktinnstillingene for de forskjellige Windows-brukerkontoene. Vi anbefaler at du konfigurerer separate Windows-brukerkontoer for hver person som bruker datamaskinen. Gjestebrukere bør for eksempel ikke ha administrative rettigheter til sine Windows-brukerkontoer.

Hvordan kjøre vanlige oppgaver

Du kan se hva du kan gjøre med produktet og kjøre vanlige oppgaver på **Oppgaver**-siden.

Slik åpner du **Oppgaver**-siden:

Klikk på **Verktøy** på hovedsiden.

Oppgaver-siden åpnes.

Slik beskytter du forskjellige brukerkontoer

For å få best mulig beskyttelse mot trusler på nettet bør du bruke separate Windows-brukerkontoer for hver person som bruker datamaskinen.

Med produktet kan du bruke forskjellige innstillinger for hver Windows-brukerkonto du har konfigurert på datamaskinen. Det er bare brukere med administratortilgang som kan endre produktinnstillingene for andre brukerkontoer. Alle andre enn administratorer bør bare ha vanlige tilgangsrettigheter slik at de ikke kan endre innstillingene du har definert for dem.

Opprette og redigere Windows-brukerkontoer

Du kan få tilgang til innstillingene for Windows-brukerkontoer gjennom produktet.

Slik oppretter eller redigerer du Windows-brukerkontoer:

1. Klikk på **Verktøy** på hovedsiden.
2. Klikk på **Opprett ny konto** eller **Rediger brukerkontoer**.
   Dette åpner brukerkontoinnstillingene i Windows.
3. Fyll inn de nødvendige opplysningene for å opprette eller redigere brukerkontoen.

Hva er nettleserbeskyttelse

Nettleserbeskyttelse hjelper deg med å evaluere sikkerheten på nettsteder du besøker, og hindrer at du utilsiktet besøker skadelige nettsteder.

Nettleserbeskyttelse er en tilleggsmodul i nettleseren, og viser sikkerhetsvurderinger av nettsteder som er oppført i resultater fra søkemotorer. Ved å hjelpe deg med å unngå nettsteder som inneholder sikkerhetstrusler, som skadelig programvare (virus, ormer, trojanere) og phishing, vil nettleserbeskyttelsens sikkerhetsvurderinger hjelpe deg med å unngå de nyeste Internett-truslene som ennå ikke er oppdaget av tradisjonelle antivirusprogrammer.

Det er fire mulige sikkerhetsvurderinger for nettsteder: sikkert, mistenkelig, skadelig og ukjent. Disse sikkerhetsvurderingene er basert på informasjon fra flere kilder, som F-Secure-analytikere og F-Secure-partnere, samt vurderinger som er gitt av andre brukere av nettleserbeskyttelsen.

Hvordan slå nettleserbeskyttelse på eller av

Når nettleserbeskyttelsen er slått på, vil tilgang til skadelige nettsteder bli blokkert.

Slik slår du nettleserbeskyttelsen på eller av:

1. Klikk på **Brukere** på hovedsiden.

2. Velg Windows-brukerkontoen du vil redigere, og klikk på bryteren ved siden av **Nettleserbeskyttelse**. Nettleserbeskyttelse blir nå slått på eller av, avhengig av forrige innstilling.
3. Hvis nettleseren er åpen, må du starte den på nytt for at den endrede innstillingen skal tre i kraft.

Sikkerhetsvurderinger i Nettleserbeskyttelse

Nettleserbeskyttelse viser sikkerhetsvurderinger for resultater fra søkemotorer.

Fargekodede ikoner viser sikkerhetsvurderingen av gjeldende nettsted (på verktøylinjen). Sikkerhetsvurderingen av hver lenke i resultater fra søkemotorer vises også med de samme ikonene. Det brukes fire forskjellige fargekodede ikoner:

- Grønt viser at siden er sikker.
- Gult viser at siden er mistenkelig. Sikkerhetsanalyse av siden angir at den er sikker, men mange brukere har gitt den en lav sikkerhetsvurdering.
- Rødt viser at siden er skadelig.
- Grått angir at siden ennå ikke er analysert og det ikke er noen tilgjengelig informasjon om den.

Sikkerhetsvurderinger er tilgjengelig på følgende søkesteder:

- Google
- MSN Live
- Yahoo

Avhengig av innstillingene for nettleserbeskyttelsen kan du besøke nettsteder som er vurdert som usikre. Nettstedene blir enten blokkert automatisk, eller du får bare en melding om mulig risiko.

Vise vurderinger av weblenker

Vurderinger fra Nettleserbeskyttelse kan vises for resultater fra søkemotorer.

Slik angir du hvor vurderingene skal vises:

1. Klikk på **Brukere** på hovedsiden.
2. Velg Windows-brukerkontoen du vil redigere, og klikk på **Innstillinger** ved siden av **Nettleserbeskyttelse**. Dialogboksen med innstillinger for **Nettleserbeskyttelse** åpnes.
3. Under **Vis vurderinger** merker du eller fjerner merkingen av **Søkemotorresultater (Google, Yahoo)**. Når dette er valgt, vil det vises vurderinger av nettstedene som er oppført i søkeresultater (fra Google, Yahoo osv.).
4. Klikk på **OK**.

Sikkerhetsvurderinger vil vises i henhold til innstillingene du har valgt.

Tips: Du kan klikke på **Sikkerhetssammendrag for dette nettstedet** i popoup-vinduet med sikkerhetsvurdering for å gå til Nettleserbeskyttelse-portalen. Der vil du finne mer informasjon om nettstedet og om hva sikkerhetsvurderingen er basert på.

Hvordan vurdere nettsteder

Du kan vurdere et nettsted du besøker, som sikkert eller skadelig.

Slik vurderer du et nettsted:

1. Velg **Varsle oss** fra nettleserbeskyttelse-menyen i nettleseren. Dette åpner dialogboksen **Varsle oss**.
2. Velg en vurdering for å gi din mening om nettstedets sikkerhet (**Det er sikkert å bruke** , **Det er skadelig å bruke** eller **Jeg har ingen mening**).
3. Klikk på **OK**.

Dette vil åpne dialogboksen med vurderingsbekreftelse.

Tips: Velg **Ikke vis denne meldingen igjen** hvis du ikke vil se bekreftelsesdialogboksen når du senere vurderer nettsteder.

4. Klikk på **OK**.

Vurderingen din sendes nå til analyse- og innsamlingsinformasjonen for dette nettstedet.

Beskytte mot skadelig innhold

Nettleserbeskyttelse blokkerer tilgang til usikre nettsteder basert på de valgte innstillingene.

Slik velger du når tilgang til et nettsted skal blokkeres:

1. Klikk på **Brukere** på hovedsiden.
2. Velg Windows-brukerkontoen du vil redigere, og klikk på **Innstillinger** ved siden av **Nettleserbeskyttelse**. Dialogboksen med innstillinger for **Nettleserbeskyttelse** åpnes.
3. Velg **Nettsteder som er vurdert som skadelige** for å blokkere tilgang til alle nettsteder som er vurdert som skadelige.
4. Klikk på **OK**.

Nettleserbeskyttelse vil nå blokkere tilgang til nettsteder i samsvar med innstillingene som er valgt.

Hva når et nettsted er blokkert

En blokkeringsside vises når du prøver å besøke et nettsted som er vurdert som skadelig.

Når en blokkeringsside vises:

1. Klikk på **Hjemmeside** for å gå til hjemmesiden uten å åpne det skadelige nettstedet.
   Vi anbefaler denne handlingen på det sterkeste.

   Tips: Du kan klikke på **Sikkerhetssammendrag for dette nettstedet** for å gå til Nettleserbeskyttelse-portalen der du vil finne mer informasjon om nettstedet og om hva sikkerhetsvurderingen er basert på.

2. Hvis du vil åpne nettstedet uansett, klikker du på **Gå til nettsted**.

Sikkerhetssammendrag for et nettsted

Et sammendrag av vurderingsinformasjonen for et vurdet nettsted er tilgjengelig på Nettleserbeskyttelse-portalen.

Sikkerhetssammendraget for et nettsted gir deg mer informasjon om hva sikkerhetsvurderingen er basert på. Sikkerhetssammendraget kan for eksempel vise om sikkerhetsvurderingen er basert på skadelig programvare som er funnet på nettstedet, lave vurderinger fra andre brukere eller begge deler. Du får tilgang til sikkerhetssammendraget fra forskjellige steder:

- Fra sikkerhetsvurderingsmenyen på verktøylinjen,
- Fra sikkerhetsvurderingsvinduet som vises for nettsstedslenker og
- Fra sikkerhetssammendragslenken på sider som er blokkert av nettleserbeskyttelsen.

Hvis du klikker på en av disse lenkene, kommer du til Nettleserbeskyttelse-portalen der du kan se informasjon om sikkerhetsvurderingen av nettstedet.

Gjøre nettbruk sikker

Du kan være trygg for mange av truslene på Internett ved å overvåke nettlesingen til alle Windows-brukerkontoene på datamaskinen.

Internett er full av interessante nettsteder, men det er også mange risikoer for alle som bruker Internett. Mange nettsteder inneholder materiale som du kanskje synes er upassende. Personer kan eksponeres for upassende materiale, eller de kan motta plagsomme meldinger via e-post eller chat. De kan ved et uhell laste ned filer som inneholder *virus* som kan skade datamaskinen.

Merk: Begrensing av tilgang til Internett-innhold beskytter brukerkontoene mot chatte- og e-postprogrammer som kjører i nettleseren. Du kan blokkere tilgang til andre chatte- eller e-postprogrammer ved å bruke sikkerhetskomponenten Programkontroll.

Du kan begrense hvilke nettsider som kan vises, og fastsette tiden du tillater brukt på Internett. Disse restriksjonene brukes på Windows-brukerkontoer, så når noen logger på med sin egen brukerkonto, gjelder restriksjonene.

Begrense tilgang til Internett-innhold

Du kan velge hvilken type filtrering du vil bruke for de forskjellige Windows-brukerkontoene.

Nettsidefiltrering vil blokkere tilgang til nettsider som du ikke har tillatt, eller til nettsider med innhold som du har bestemt deg for å blokkere.

Tillate nettsider

Du kan tillate tilgang bare til nettsteder og -sider du stoler på, ved å legge dem til listen over tillatte nettsteder.

Slik tillater du spesifikke nettsider:

1. Klikk på **Brukere** på hovedsiden.
2. Velg Windows-brukerkontoen du vil redigere, og klikk på **Innstillinger** ved siden av **Websidefilter**. Webfiltrering-veiviseren åpnes.
3. Klikk på **Neste** på den første siden.
4. Velg **Tillat bare valgte nettsteder** og klikk på **Neste**.
5. Klikk på **Legg til** for å legge til nettsteder på listen **Tillatte nettsteder**.
6. Når du har lagt til alle nettstedene du vil tillate, klikker du på **Neste**.
7. Klikk på **Fullfør** for å lukke veiviseren for webfiltrering.

Alle som bruker Windows-kontoen du redigerte, kan nå bare åpne nettsteder som du la til på listen over tillatte nettsteder.

Blokkere nettsider etter innholdstype

Med nettsidefilteret kan du tillate, blokkere eller bare logge tilgang til nettsteder og -sider.

Slik velger du hvilket innhold du vil tillate:

1. Klikk på **Brukere** på hovedsiden.
2. Velg Windows-brukerkontoen du vil redigere, og klikk på **Innstillinger** ved siden av **Websidefilter**. Webfiltrering-veiviseren åpnes.
3. Klikk på **Neste** på den første siden.
4. Velg **Begrens nettlesing etter innhold** og klikk på **Neste**.
5. På siden **Begrens Internett-innhold** velger du typen innhold du vil blokkere.
6. Når du har valgt alle innholdstypene du vil blokkere, klikker du på **Neste**.

7. Klikk på **Fullfør** for å lukke veiviseren for webfiltrering.

Alle som bruker Windows-kontoen du redigerte, vil ikke få tilgang til nettsteder med innhold som du har blokkert.

Redigering tillatt og blokkerte nettsteder

Du kan velge å tillate spesifikke nettsteder som er blokkert av webfiltrering, og også blokkere individuelle nettsteder som ikke er inkludert i noen innholdstype for webfiltrering.

Du kan for eksempel anse et nettsted som sikkert, selv om du vil blokkere andre nettsteder med samme innholdstype. Du kan også blokkere et spesifikt nettsted selv om andre nettsteder med samme innholdstype, er tillatt.

Slik tillater eller blokkerer du et nettsted:

1. Klikk på **Brukere** på hovedsiden.
2. Velg Windows-brukerkontoen du vil redigere, og klikk på **Åpne nettstedsliste**.

   Hvis nettstedet du vil redigere, allerede er oppført som tillatt eller forbudt, og du vil flytte det fra den ene listen til den andre:

   a) Avhengig av hvilken nettstedsliste du vil redigere, klikker du på kategorien **Tillatt** eller **Forbudt**.
   b) Høyreklikk på nettstedet på listen, og velg deretter **Tillat** eller **Forby**.

   Hvis nettstedet ikke er oppført på noen av listene:

   a) Klikk på kategorien **Tillat** hvis du vil tillate et nettsted, eller klikk på kategorien **Forby** hvis du vil blokkere et nettsted.
   b) Klikk på **Legg til** for å legge til det nye nettstedet på listen.
   c) I dialogboksen **Legg til nettsted** skriver du adressen til nettstedet du vil legge til. Klikk deretter på **OK**.
3. Klikk på **Lukk** for å gå tilbake til hovedsiden.

Hvis du skal endre adressen til et tillatt eller blokkert nettsted, høyreklikker du på nettstedet i listen og velger **Rediger**.

Hvis du vil fjerne et tillatt eller blokkert nettsted fra listen, velger du nettstedet og klikker på **Fjern**.

Hvordan angi surfetid

Du kan bestemme tidsperiodene som kan brukes til å surfe på Internett på datamaskinen.

Du kan angi forskjellige restriksjoner for hver Windows-brukerkonto på datamaskinen. Du kan styre:

- Når noen får lov til å surfe på Internett. Du kan for eksempel tillate surfing på Internett bare før 20.00 om kvelden.
- Hvor lenge noen kan bruke på Internett. Du kan for eksempel tillate bruk av Internett bare én time om dagen.

Merk: Hvis du fjerner tidsbegrensningene, kan Internett brukes uten tidsbegrensninger.

Når tidsrestriksjonene blokkerer tilgang til Internett, vil en blokkeringsside i nettleseren angi når Internett kan brukes igjen. Hvis din Windows-brukerkonto har administrative rettigheter, kan du forlenge nettlesertiden ved å angi passordet for din Windows-brukerkonto og angi mer tid.

Begrense daglig surfetid

Du kan bruke daglige tidsgrenser til å begrense tilgangen til Internett.

Du kan angi forskjellige daglige tidsgrenser for hver Windows-brukerkonto på datamaskinen.

Slik angir du tidsgrensene:

1. Klikk på **Brukere** på hovedsiden.
2. Velg Windows-brukerkontoen du vil redigere, og klikk på **Innstillinger** ved siden av **Tidsgrenser**. Veiviseren **Begrens nettlesertid** åpnes.
3. Klikk på **Neste** på den første siden.
4. I tabellen **Tillatte nettlesertimer** velger du tidspunktene når nettlesing er tillatt for hver dag i uken.
5. Når du har angitt tillatt nettlesertid, klikker du på **Neste**.
6. Velg hvor mange timer Internett-bruk som er tillatt på ukedager og i helger, og klikk deretter på **Neste**.
7. Klikk på **Fullfør** for å lukke veiviseren.

Alle som bruker Windows-kontoen du redigerte, kan nå bare bruke Internett innenfor de tillatte tidspunktene.

Vise statistikk

Du kan se hvilke nettsider som har blitt vist og hvilke som er blokkert, på **Statistikk**-siden.

Produktet samler inn informasjon om besøkte og blokkerte nettsteder. Denne informasjonen er brukerspesifikk for hver Windows-brukerkonto.

Blokkerte nettsteder inndeles i steder som er blokkert av websidefiltrering, og steder som er blokkert av nettleserbeskyttelse. Dette viser deg om et nettsted har innhold som du har blokkert, eller om produktet har identifisert det som et mulig skadelig nettsted.