F-Secure Anti-Virus 2013

Indhold

Kapitel 1: Installation.....5

Før du installerer for første gang.....6
Installere produktet for første gang.....6
Installere og opgradere programmer.....6
Hjælp og support.....7

Kapitel 2: Introduktion.....9

Bruge automatiske opdateringer.....10
Kontrollere opdateringsstatus.....10
Ændre indstillingerne for din internetforbindelse.....10
Kontroller status for realtidsbeskyttelsesnetværket.....11
Hvordan ser jeg, hvad produktet har gjort.....11
Vise beskedoversigten.....11
Ændre indstillinger for beskeder.....11
Realtidsbeskyttelsesnetværk.....12
Hvad er realtidsbeskyttelsesnetværket.....12
Fordele ved realtidsbeskyttelsesnetværket.....12
Hvilke data du bidrager med.....13
Sådan beskytter vi dine personlige oplysninger.....14
Sådan bliver du bidragyder til realtidsbeskyttelsesnetværket.....14
Spørgsmål om realtidsbeskyttelsesnetværk.....14
Hvordan ved jeg, at mit abonnement er gyldigt.....15
Handlingscenter.....15
Aktivere et abonnement.....15

Kapitel 3: Introduktion.....17

Få vist den generelle status for min beskyttelse.....18
Vise produktstatistikken.....18
Håndtere produktopdateringer.....19
Vise databaseversioner.....19
Redigere indstillingerne for mobilt bredbånd.....19
Hvad er virus og anden malware.....20
Virus.....20
Spyware.....20
Rootkits.....21
Riskware.....21

Kapitel 4: Beskyttelse af computeren mod malware.....23
Sådan scannes min computer.....24
Scanne filer automatisk.....24
Scanne filer manuelt.....26
Scanne e-mails.....29
Vise scanningsresultaterne.....29
Sådan udelades filer fra scanningen.....30
Udelad filtyper.....30
Udelad filer efter placering.....30
Vis udeladte programmer.....31
Sådan anvendes karantæne.....32
Vis elementer i karantæne.....32
Gendan elementer i karantæne.....32
Hvad er DeepGuard?.....33
Slå DeepGuard til eller fra.....33
Tillade programmer, som DeepGuard har blokeret.....33
Bruge DeepGuard i kompatibilitetstilstand.....34
Gør følgende med advarsler om mistænkelig adfærd.....34

Kapitel

1

Installation

Emner:

- *Før du installerer for første gang*
- *Installere produktet for første gang*
- *Installere og opgradere programmer*
- *Hjælp og support*

Før du installerer for første gang

Tak, fordi du valgte F-Secure.

Du skal bruge følgende for at installere produktet:

- Installations-cd'en eller en installationspakke. Hvis du bruger en netbookcomputer uden et cd-drev, kan du hente installationspakken fra *www.f-secure.com/netbook*.
- Din abonnementsnøgle.
- En internetforbindelse.

Hvis du har et sikkerhedsprodukt fra en anden leverandør, forsøger installationsprogrammet at fjerne det automatisk. Hvis det ikke lykkedes, skal du fjerne det manuelt.

Bemærk: Hvis du har mere end én konto på computeren, skal du logge på med administratorrettigheder, når du installerer.

Installere produktet for første gang

Anvisninger i installation af produktet.

Følg disse anvisninger for at installere produktet:

1. Indsæt cd'en, eller dobbeltklik på installationsprogrammet, du hentede.

   Hvis cd'en ikke starter automatisk, skal du gå til Windows Stifinder, dobbeltklikke på cd-rom-ikonet og dobbeltklikke på installationsfilen for at starte installationen.

2. Følg anvisningerne på skærmen.

   - Hvis du købte produktet på en cd i en forretning, kan du finde abonnementsnøglen på omslaget til installationsvejledningen.
   - Hvis du hentede produktet fra F-Secure eStore, medfølger abonnementsnøglen i e-mailen til bekræftelse af købsordren.

   Computeren skal genstartes, inden du validerer abonnementet eller henter de nyeste opdateringer fra internettet. Hvis du installerer fra cd'en, skal du huske at fjerne installations-cd'en, før du genstarter computeren.

Installere og opgradere programmer

Anvisninger i aktivering af dit nye abonnement.

Følg disse anvisninger for at aktive dit nye abonnement eller installlere et nyt program ved hjælp af startområdet:

Bemærk: Du kan finde ikonet for startområdet på proceslinjen i Windows.

1. Højreklik på ikonet længst til højre i startområdet.
   Der åbnes en pop op-menu.
2. Vælg **Vis mine abonnementer**
3. Gå tll siden **Abonnementsstatus** under **Mine abonnementer**, og klik på **Aktiver abonnement**.
   Vinduet **Aktiver abonnement** åbnes.

4. Indtast abonnementsnøglen til programmet, og klik på **OK**.
5. Når abonnementet er valideret og aktiveret, skal du klikke på **Luk**.
6. Gå til siden **Installationsstatus** under **Mine abonnementer**. Hvis installationen ikke starter automatisk, skal du følge disse anvisninger:
   a) Klik på **Installer**.
   Installationsvinduet åbnes.
   b) Klik på **Næste**.
   Programmet hentes, og installationen begynder.
   c) Når installationen er afsluttet, skal du klikke på **Luk**.

Det nye abonnement er blevet aktiveret.

Hjælp og support

Du kan få adgang til produktets onlinehjælp ved at klikke på ikonet Hjælp eller ved at trykke på F1 på et hvilket som helst skærmbilledet i produktet.

Når du har registreret din licens, er du berettiget til yderligere tjenester som f.eks. gratis produktopdateringer og produktsupport. Du kan registrere produktet på *www.f-secure.com/register*.

Kapitel

2

Introduktion

Emner:

- *Bruge automatiske opdateringer*
- *Hvordan ser jeg, hvad produktet har gjort*
- *Realtidsbeskyttelsesnetværk*
- *Hvordan ved jeg, at mit abonnement er gyldigt*

Oplysninger om, hvordan man kommer i gang med produktet.

I dette afsnit beskrives, hvordan du ændrer fælles indstillinger og administrerer dine abonnementer via startområdet.

Startområdets fælles indstillinger er indstillinger, som gælder for alle programmer, der er installeret i startområdet. I stedet for at ændre indstillingerne i hvert enkelt program, kan du blot redigere de fælles indstillinger, som bruges af alle de installerede programmer.

Startområdets fælles indstillinger omfatter:

- Overførsler, hvor du kan få vist oplysninger om, hvilke opdateringer der er blevet overført, og manuelt kontrollere, om der er nye opdateringer.
- Forbindelsesindstillinger, hvor du kan ændre, hvordan computeren opretter forbindelse til internettet.
- Beskeder, hvor du kan få vist tidligere beskeder og angive, hvilke typer beskeder du vil se.
- Indstillinger for beskyttelse af private oplysninger, hvor du kan vælge, om computeren må oprette forbindelse til realtidsbeskyttelsesnetværket.

Du kan også administrere dine abonnementer på installerede programmer via startområdet.

Bruge automatiske opdateringer

Automatiske opdateringer sørger for, at beskyttelsen på din computer er opdateret.

Produktet henter de seneste opdateringer til din computer, når du har oprettet forbindelse til internettet. Det registrerer netværkstrafikken og forstyrrer ikke anden internetbrug, selv ved en langsom netværksforbindelse.

Kontrollere opdateringsstatus

Få vist dato og tidspunkt for den seneste opdatering.

Hvis automatiske opdateringer er slået til, modtager produktet automatisk de seneste opdateringer, hvis du er har forbindelse til internettet.

For at sikre, at du har de seneste opdateringer:

1. Højreklik på ikonet længst til højre i startområdet.
   Der vises en pop op-menu.
2. Vælg **Åbn generelle indstillinger**.
3. Vælg **Automatiske opdateringer** > **Overførsler**.
4. Klik på **Kontroller nu**.
   Produktet opretter forbindelse til internettet og søger efter de seneste opdateringer. Hvis beskyttelsen ikke er opdateret, henter den de seneste opdateringer.

   Bemærk: Hvis du bruger et modem eller har en ISDN-forbindelse til internettet, skal forbindelsen være aktiv for, at du kan kontrollere, om der er opdateringer.

Ændre indstillingerne for din internetforbindelse

Der er normalt ikke behov for at ændre standardindstillingerne, men du kan konfigurere, hvordan serveren har forbindelse til internettet, så du kan modtage opdateringer automatisk.

Sådan ændres indstillingerne for din internetforbindelse:

1. Højreklik på ikonet længst til højre i startområdet.
   Der vises en pop op-menu.
2. Vælg **Åbn generelle indstillinger**.
3. Vælg **Automatiske opdateringer** > **Forbindelse**.
4. Vælg, hvordan din computer har forbindelse til internettet, på listen **Internetforbindelse**.
   - Vælg **Antag, der altid er forbindelse**, hvis du har en permanent netværksforbindelse.

     Bemærk: Hvis din computer rent faktisk ikke har en permanent netværksforbindelse og er konfigureret til opkald efter behov, og du vælger **Antag, der altid er forbindelse**, kan det resultere i flere opkald.
   - Vælg **Registrer forbindelse** for at hente opdateringer, når produktet registrerer en aktiv netværksforbindelse.
   - Vælg **Registrer trafik** for kun at hente opdateringer, når produktet registrerer anden netværkstrafik.

     Tip: Hvis du har en usædvanlig hardwarekonfiguration, som gør, at indstillingen **Registrer forbindelse** registrerer en aktiv netværksforbindelse, selvom der ikke er nogen, skal du vælge **Registrer trafik** i stedet.
5. Vælg på listen **HTTP-proxy**, om din computer bruger en *proxyserver* til at oprette forbindelse til internettet.

- Vælg **Ingen HTTP-proxy**, hvis din computer har direkte forbindelse til internettet.
- Vælg **Konfigurer HTTP-proxy manuelt** for at konfigurere *HTTP-proxy*-indstillingerne.
- Vælg **Brug min browsers HTTP-proxy** for at bruge de samme *HTTP-proxy-indstillinger*, som du har konfigureret i din webbrowser.

Kontroller status for realtidsbeskyttelsesnetværket

Mange produktfunktioner afhænger af forbindelse til realtidsbeskyttelsesnetværket for at fungere korrekt.

Hvis der er netværksproblemer, eller hvis din firewall blokerer trafikken til og fra realtidsbeskytttelsesnetværket, er statussen 'afbrudt'. Hvis der ikke er installeret produktfunktioner, som kræver adgang til realtidsbeskyttelsesnetværket, er statussen 'ikke i brug'.

Sådan kontrolleres status:

1. Højreklik på ikonet længst til højre i startområdet.
   Der vises en pop op-menu.
2. Vælg **Åbn generelle indstillinger**.
3. Vælg **Automatiske opdateringer** > **Forbindelse**.

Under **Realtidsbeskyttelsesnetværk** kan du se den aktuelle status for realtidsbeskyttelsesnetværket.

Hvordan ser jeg, hvad produktet har gjort

Du kan se, hvilke handlinger produktet har foretaget for at beskytte din computer, på siden **Beskeder**.

Produktet viser en besked, når det foretager en handling, eksempelvis når det finder en virus, som blokeres. Visse beskeder kan også blive sendt til dig af din tjenesteudbyder for at give dig besked om nye tjenester, der er tilgængelige.

Vise beskedoversigten

Du kan se, hvilke beskeder der er blevet vist, i beskedoversigten.

Sådan vises beskedoversigten:

1. Højreklik på ikonet længst til højre i startområdet.
   Der vises en pop op-menu.
2. Vælg **Åbn generelle indstillinger**.
3. Vælg **Andet** > **Beskeder**.
4. Klik på **Vis beskedoversigt**.
   Beskedoversigten åbnes.

Ændre indstillinger for beskeder

Du kan vælge, hvilke typer beskeder produktet skal vise.

Sådan ændres indstillinger for beskeder:

1. Højreklik på ikonet længst til højre i startområdet.
   Der vises en pop op-menu.
2. Vælg **Åbn generelle indstillinger**.
3. Vælg **Andet** > **Beskeder**.

4. Marker eller fjern markeringen i feltet **Tillad programmeddelelser** for at slå programmeddelelser til eller fra.

   Når denne indstilling er slået fra, viser produktet beskeder fra de installerede programmer.

5. Marker eller fjern markeringen i feltet **Tillad reklamemeddelelser** for at slå reklamemeddelelser til eller fra.
6. Klik på **OK**.

Realtidsbeskyttelsesnetværk

I dette dokument beskrives realtidsbeskyttelsesnetværket, en onlinetjeneste fra F-Secure Corporation, som identificerer "rene" programmer og websteder og samtidig yder beskyttelse mod malware og sikkerhedsrisici på websteder.

Hvad er realtidsbeskyttelsesnetværket

Realtidsbeskyttelsesnetværket er en onlinetjeneste, som reagerer hurtigt på de seneste internetbaserede trusler.

Som bidragyder til realtidsbeskyttelsesnetværket kan du hjælpe os med at styrke beskyttelsen mod nye trusler, der dukker op. Realtidsbeskyttelsesnetværket indsamler statistiske oplysninger om visse ukendte, ondsindede eller mistænkelige programmer, og hvad de gør på din enhed. Disse oplysninger er anonyme og sendes til F-Secure Corporation med henblik på kombineret dataanalyse. Vi bruger de analyserede oplysninger til at forbedre sikkerheden på enheden mod de nyeste trusler og ondsindede filer.

Sådan fungerer realtidsbeskyttelsesnetværket

Som bidragyder til realtidsbeskyttelsesnetværket kan du give oplysninger om ukendte programmer og websteder samt om ondsindede programmer og sårbarheder på websteder. Realtidsbeskyttelsesnetværket sporer ikke dine internetaktiviteter og indsamler ikke oplysninger om websteder, som allerede er blevet analyseret, og det indsamler ikke oplysninger om installerede programmer på computeren, der ikke er inficeret.

Hvis du ikke ønsker at bidrage med disse data, indsamler realtidsbeskyttelsesnetværket ikke oplysninger om installerede programmer eller besøgte websteder. Men produktet skal sende forespørgsler til F-Secure-servere angående programmers, websteders, meddelelsers og andre objekters omdømme. Forespørgslen udføres ved hjælp af en kryptografisk kontrolsum, hvor selve det objekt, der forespørges om, ikke sendes til F-Secure. Vi sporer ikke data pr. bruger, og det er kun tællerværdien for filen eller webstedet der forøges.

Det er ikke muligt fuldstændigt at standse al trafik til realtidsbeskyttelsesnetværket, da det er en integreret del af beskyttelsen, som produktet yder.

Fordele ved realtidsbeskyttelsesnetværket

Med realtidsbeskyttelsesnetværket får du hurtigere og mere nøjagtig beskyttelse mod de nyeste trusler, og du modtager ikke unødvendige beskeder om mistænkelige programmer, som ikke er ondsindede.

Som bidragyder til realtidsbeskyttelsesnetværket kan du hjælpe os med at finde ny og endnu ikke opdaget malware samt fjerne mulige falske positiver fra vores virusdefinitionsdatabase.

Alle deltagere i realtidsbeskyttelsesnetværket hjælper hinanden. Når realtidsbeskyttelsesnetværket finder et mistænkeligt program på din enhed, nyder du godt af analyseresultaterne, hvis det samme program allerede er blevet fundet på andre enheder. Realtidsbeskyttelsesnetværket forbedrer din enheds overordnede ydelse, da det installerede sikkerhedsprodukt ikke behøver at scanne de programmer igen, som realtidsbeskyttelsesnetværket har analyseret og fundet sikre. På lignende vis deles oplysninger om ondsindede websteder og uønskede massemeddelelser via realtidsbeskyttelsesnetværket, og vi er i stand til at give dig mere nøjagtig beskyttelse mod sikkerhedsrisici på websteder og spammeddelelser.

Jo flere personer, der bidrager til realtidsbeskyttelsesnetværket, desto bedre er individuelle deltagere beskyttet.

Hvilke data du bidrager med

Som bidragyder til realtidsbeskyttelsesnetværket leverer du oplysninger om programmer på din enhed og de websteder, som du besøger, så realtidsbeskyttelsesnetværket kan yde beskyttelse mod de nyeste ondsindede programmer og mistænkelige websteder.

Analysere filernes omdømme

Realtidsbeskyttelsesnetværket indsamler kun oplysninger om programmer, som ikke har et kendt omdømme, og om filer, der er mistænkelige eller vides at være malware.

Realtidsbeskyttelsesnetværket indsamler anonyme oplysninger om "rene" og mistænkelige programmer på din enhed. Realtidsbeskyttelsesnetværket indsamler kun oplysninger om eksekverbare filer (f.eks. flytbare eksekverbare filer på Windows-platformen med filtypenavnene .cpl, .exe, .dll, .ocx, .sys, .scr og .drv).

De indsamlede oplysninger omfatter:

- filstien, hvor programmet befinder sig på enheden,
- størrelsen på filen og hvornår den blev oprettet eller ændret,
- filattributter og -rettigheder,
- oplysninger om filsignatur,
- filens aktuelle version og virksomheden, som oprettede den,
- filens oprindelse eller URL-adressen til hentning,
- analyseresultater af scannede filer fra F-Secure DeepGuard og antivirus og
- andre tilsvarende oplysninger.

Realtidsbeskyttelsesnetværket indsamler aldrig oplysninger om dine personlige dokumenter, medmindre de er inficerede. For alle typer ondsindede filer indsamles navnet på inficeringen og filens desinficeringsstatus.

Med realtidsbeskyttelsesnetværket kan du også indsende mistænkelige programmer til analyse. Indsendte programmer omfatter kun flytbare, eksekverbare filer. Realtidsbeskyttelsesnetværket indsamler aldrig oplysninger om dine personlige dokumenter, og de overføres aldrig automatisk til analyse.

Indsende filer til analyse

Med realtidsbeskyttelsesnetværket kan du også indsende mistænkelige programmer til analyse.

Du kan sende enkelte mistænkelige programmer manuelt, når produktet beder dig om at gøre det. Du kan kun sende flytbare, eksekverbare filer. Realtidsbeskyttelsesnetværket overfører aldrig dine personlige dokumenter.

Analysere websteders omdømme

Realtidsbeskyttelsesnetværket sporer ikke din webaktivitet og indsamler heller ikke oplysninger om websteder, der allerede er blevet analyseret. Det sikrer, at besøgte websteder er sikre, når du søger på internettet. Når du besøger et websted, undersøger realtidsbeskyttelsesnetværket webstedets sikkerhed og giver dig besked, hvis webstedet vurderes som mistænkeligt eller skadeligt.

Hvis det websted, du besøger, indeholder ondsindet eller mistænkeligt indhold eller en kendt sikkerhedsrisiko, indsamler realtidsbeskyttelsesnetværket hele URL-adressen på webstedet, så websideindholdet kan analyseres.

Hvis du besøger et websted, der endnu ikke er blevet klassificeret, indsamler realtidsbeskyttelsesnetværket domæne- og underdomænenavne og i nogle tilfælde stien til den besøgte side, så webstedet kan analyseres og klassificeres. Alle de URL-parametre, der sandsynligvis indeholder oplysninger, som kan forbindes med dig i et personligt og identificerbart format, fjernes for at beskytte dine personlige oplysninger.

Bemærk: Realtidsbeskyttelsesnetværket vurderer eller analyserer ikke websider på private netværk, så der indsamles aldrig oplysninger om private IP-netværksadresser (f.eks. virksomheders intranet).

Analysere systemoplysningerne

Realtidsbeskyttelsesnetværket indsamler navnet på og versionen af dit operativsystem, oplysninger om internetforbindelsen og brugsstatistik for realtidsbeskyttelsesnetværket (f.eks. hvor mange gange der er forespurgt om et websteds omdømme og den gennemsnitlige tid, det tager at returnere et resultat), så vi kan overvåge og forbedre tjenesten.

Sådan beskytter vi dine personlige oplysninger

Vi overfører oplysningerne sikkert og fjerner automatisk personlige oplysninger, som dataene kan indeholde.

Realtidsbeskyttelsesnetværket fjerner identificerende data, inden de sendes til F-Secure, og det krypterer alle indsamlede oplysninger under overførslen for at beskytte dem mod uautoriseret adgang. De indsamlede oplysninger behandles ikke enkeltvist, men grupperes sammen med oplysninger fra andre bidragydere til realtidsbeskyttelsesnetværket. Alle data analyseres statistisk og anonymt, hvilket betyder, at ingen data på nogen måde knyttes til dig.

Oplysninger, som kan identificere dig personligt, medtages ikke i de indsamlede data. Realtidsbeskyttelsesnetværket indsamler ikke private IP-adresser eller dine private oplysninger som f.eks. e-mail-adresser, brugernavne og adgangskoder. Selvom vi gør os alle bestræbelser på at fjerne personligt identificerbare data, er det muligt, at der fortsat vil være nogle identificerende data i de indsamlede oplysninger. I sådanne tilfælde forsøger vi ikke at bruge disse data, der er indsamlet utilsigtet, til at identificere dig.

Vi anvender strenge sikkerhedsforanstaltninger og fysiske, administrative og tekniske beskyttelsesordninger for at beskytte de indsamlede oplysninger, når de overføres, gemmes og behandles. Oplysningerne gemmes på sikre steder og på servere, der kontrolleres af os, og som befinder sig enten på vores kontorer eller vores underleverandørers kontorer. Kun autoriseret personale kan få adgang til de indsamlede oplysninger.

F-Secure kan dele de indsamlede data med datterselskaber, underleverandører, distributører og partnere, men altid i et anonymt format, der ikke kan identificeres.

Sådan bliver du bidragyder til realtidsbeskyttelsesnetværket

Du kan hjælpe os med at forbedre beskyttelsen i realtidsbeskyttelsesnetværket ved at bidrage med oplysninger om ondsindede programmer og websteder.

Du kan vælge at blive deltager i realtidsbeskyttelsesnetværket under installationen. Med indstillingerne for standardinstallationen bidrager du med data til realtidsbeskyttelsesnetværket. Du kan ændre denne indstilling i produktet senere.

Følg disse instruktioner for at ændre indstillinger for realtidsbeskyttelsesnetværket:

1. Højreklik på ikonet længst til højre i startområdet.
   Der vises en pop op-menu.
2. Vælg **Åbn generelle indstillinger**.
3. Vælg **Andet** > **Beskyttelse af personlige oplysninger**.
4. Marker deltagerafkrydsningsfeltet for at blive bidragyder til realtidsbeskyttelsesnetværket.

Spørgsmål om realtidsbeskyttelsesnetværk

Kontaktoplysninger til spørgsmål om realtidsbeskyttelsesnetværk.

Hvis du har yderligere spørgsmål om realtidsbeskyttelsesnetværket, bedes 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 version af denne politik findes altid på vores websted.

Hvordan ved jeg, at mit abonnement er gyldigt

Din abonnementstype og -status er vist på siden **Abonnementsstatus**.

Når abonnementet er ved at udløbe, eller hvis dit abonnement er udløbet, ændres programmets overordnede beskyttelsesstatus på det tilsvarende ikon i startområdet.

For at kontrollere dit abonnements gyldighed:

1. Højreklik på ikonet længst til højre i startområdet.
   Der vises en pop op-menu.
2. Vælg **Vis mine abonnementer**.
3. Vælg **Abonnementsstatus** for at få vist oplysninger om dine abonnementer på installerede programmer.
4. Vælg **Installationsstatus** for at se, hvilke programmer der kan installeres.

Abonnementsstatus og udløbsdato vises også på programsiden **Statistik**. Hvis abonnementet er udløbet, skal du forny det for at fortsætte med at modtage opdateringer og bruge produktet.

Bemærk: Når dit abonnement er udløbet, blinker produktstatusikonet på proceslinjen.

Handlingscenter

I handlingscenteret vises vigtige beskeder, der kræver din opmærksomhed.

Hvis dit abonnement er udløbet eller ved at udløbe, bliver du underrettet om det af handlingscenteret. Baggrundsfarven og indholdet af meddelelsen fra handlingscenteret afhænger af din abonnementstype og -status:

- Hvis dit abonnement er ved at udløbe, og der findes gratis abonnementer, har meddelelsen en hvid baggrund og knappen **Aktiver**.
- Hvis dit abonnement er ved at udløbe, og der ikke findes nogen gratis abonnementer, har meddelelsen en gul baggrund og knapperne **Køb** og **Indtast nøgle**. Hvis du allerede har købt et nyt abonnement, kan du klikke på **Indtast nøgle** for at angive abonnementsnøglen og aktivere dit nye abonnement.
- Hvis dit abonnement er udløbet, og der findes gratis abonnementer, har meddelelsen en rød baggrund og knappen **Aktiver**.
- Hvis dit abonnement er udløbet, og der ikke findes nogen gratis abonnementer, har meddelelsen en rød baggrund og knapperne **Køb** og **Indtast nøgle**. Hvis du allerede har købt et nyt abonnement, kan du klikke på **Indtast nøgle** for at angive abonnementsnøglen og aktivere dit nye abonnement.

Bemærk: Linket **Vis beskedoversigt** i handlingscenteret viser en liste over produktmeddelelser, ikke tidligere meddelelser fra handlingscenteret.

Aktivere et abonnement

Når du har en ny abonnementskode eller kampagnekode til et produkt, skal du aktivere den.

Sådan aktiveres et abonnement:

1. Højreklik på ikonet længst til højre i startområdet.
   Der vises en pop op-menu.
2. Vælg **Vis mine abonnementer**.
3. Vælg en af følgende:
   - Klik på **Aktiver abonnement**.
   - Klik på **Aktiver kampagnekode**.
4. Indtast din nye abonnementsnøgle eller kampagnekode i dialogboksen, der åbnes, og klik på **OK**.

   Tip: Hvis du modtog abonnementsnøglen via e-mail, kan du kopiere den fra e-mailen og indsætte den i feltet.

Når du har indtastet den nye abonnementsnøgle, vises den nye gyldighedsdato for abonnementet på siden **Abonnementsstatus**.

Kapitel

3

Introduktion

Emner:

- *Få vist den generelle status for min beskyttelse*
- *Vise produktstatistikken*
- *Håndtere produktopdateringer*
- *Hvad er virus og anden malware*

Dette produkt beskytter din computer mod virus og andre skadelige programmer.

Produktet scanner filer, analyserer programmer og opdaterer dem automatisk. Du behøver ikke foretage dig noget.

Få vist den generelle status for min beskyttelse

Siden **Status** indeholder en hurtig oversigt over installerede produktfunktioner og deres aktuelle status.

Sådan åbnes siden **Status**:

På hovedsiden skal du klikke på **Status**.

Siden **Status** åbnes.

Ikonerne viser status for programmet og dets sikkerhedsfunktioner.

Statusikon	Statusnavn	Beskrivelse
	OK	Din computer er beskyttet. Funktionen er aktiveret og fungerer korrekt.
	Information	Produktet informerer dig om en særlig status for en funktion. Eksempelvis at funktionen er ved at blive opdateret.
	Advarsel	Computeren er ikke fuldt beskyttet. Eksempelvis at produktet ikke har modtaget opdateringer i lang tid, eller at status for en funktion kræver din opmærksomhed.
	Fejl	Din computer er ikke beskyttet Eksempelvis at dit abonnement er udløbet, eller at en kritisk funktion er slået fra.
	Fra	En ikke-kritisk funktion er slået fra.

Vise produktstatistikken

Du kan se, hvad produktet har foretaget, siden installationen af det på siden **Siden Statistik**.

Sådan åbnes siden **Statistik**:

I hovedvinduet skal du klikke på **Statistik**.

Siden **Statistik** åbnes.

- **Sidste vellykkede opdateringskontrol** viser tiden for den seneste opdatering.

- **Virus- og spywarescanning** viser, hvor mange filer produktet har scannet og renset siden installationen.
- **Programmer** viser, hvor mange programmer DeepGuard har tilladt eller blokeret siden installationen.
- **Firewallforbindelser** viser antallet af tilladte og blokerede forbindelser siden installationen.
- **Filtrering af spam og phishing** viser, hvor mange e-mails produktet har registreret som gyldige e-mails og som spammeddelelser.

Håndtere produktopdateringer

Produktet holder automatisk beskyttelsen opdateret.

Vise databaseversioner

Du kan se tidspunkterne for de seneste opdateringer og versionnumre på siden **Databaseopdateringer**.

Sådan åbnes siden **Databaseopdateringer**:

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Andre indstillinger** > **Databaseversioner**.

På siden **Databaseversioner** vises den seneste dato, da virus- og spywaredefinitioner, DeepGuard og filtrering af spam og phishing blev opdateret samt deres versionsnumre.

Redigere indstillingerne for mobilt bredbånd

Vælg, om du vil hente sikkerhedsopdateringer, når du bruger mobilt bredbånd.

Bemærk: Denne funktion er kun tilgængelig i Microsoft Windows 7.

Som standard hentes sikkerhedsopdateringer altid, når du er i din hjemmeoperatørs netværk. Men opdateringerne slås midlertigt fra, når du besøger en anden operatørs netværk. Det skyldes, at forbindelsespriserne f.eks. kan variere mellem operatører i forskellige lande. Du kan overveje at lade denne indstilling være uændret, hvis du spare båndbredde, og muligvis også omkostninger, under dit besøg.

Bemærk: Denne indstilling gælder kun for mobile bredbåndsforbindelser. Når computeren er tilsluttet et fast eller trådløst netværk, opdateres produktet automatisk.

Sådan ændres indstillingen:

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Andre indstillinger** > **Mobilt bredbånd** > **Hent sikkerhedsopdateringer**.
3. Vælg den foretrukne opdateringsindstilling til mobile forbindelser:
   - **Kun i min hjemmeoperatørs netværk**

     Opdateringer hentes altid i din hjemmeoperatørs netværk. Når du besøger en anden operatørs netværk, slås opdateringerne midlertidigt fra. Det anbefales, at du vælger denne indstilling for at holde dit sikkerhedsprodukt opdateret til forventede omkostninger.
   - **Aldrig**

     Opdateringer hentes ikke, når du bruger mobilt bredbånd.
   - **Altid**

Opdateringer hentes altid, uanset hvilket netværk du bruger. Vælg denne indstilling, hvis du vil sørge for, at computerens sikkerhed altid er opdateret, uanset omkostningerne.

4. Hvis du vil bestemme, hver gang du forlader din hjemmeoperatørs netværk, skal du vælge **Spørg, hver gang du forlader din hjemmeoperatørs netværk**.

Sikkerhedsopdateringer midlertidigt slået fra

Sikkerhedsopdateringerne kan være midlertidigt slået fra, når du bruger det mobile bredbånd uden for din hjemmeoperatørs netværk.

Du kan i dette tilfælde se beskeden **Afbrudt** nederst til højre på skærmen. Opdateringerne er midlertidigt afbrudt, fordi priserne på forbindelserne eksempelvis kan variere fra operatør til operatør i forskellige lande. Du kan overveje at lade denne indstilling være uændret, hvis du vil spare båndbredde og muligvis også udgifter under dit besøg. Hvis du stadig vil ændre indstillingerne, skal du klikke på linket **Skift**.

Bemærk:

Denne funktion er kun tilgængelig i Microsoft Windows 7.

Hvad er virus og anden malware

Malware er programmer, der er specifikt konstrueret til at skade din computer, bruge din computer til ulovlige formål uden din viden eller stjæle oplysninger fra din computer.

Malware kan:

- få kontrol over din webbrowser,
- omdirigere dine søgeforsøg,
- vise uønsket annoncering,
- holde øje med de websteder, du besøger,
- stjæle personlige oplysninger såsom dine bankoplysninger,
- bruge din computer til at sende spam, og
- bruge din computer til at angribe andre computere.

Malware-programmer kan også gøre din computer langsom eller ustabil. Det kan være et tegn på, at du har *malware* på din computer, hvis den pludselig bliver meget langsom og ofte går ned.

Virus

En virus er sædvanligvis et program, der kan vedhæfte sig selv til filer og replikere sig selv gentagne gange; den kan ændre og erstatte andre filers indhold på en måde, der kan skade din computer.

En *virus* er et program, som normalt installeres på din computer uden din viden. Når den er installeret, forsøger den at replikere sig selv. Virussen:

- bruger nogle af din computers systemressourcer
- kan ændre eller skade filer på computeren,
- forsøger muligvis at bruge computeren til at inficere andre computere,
- kan tillade, at din computer bruges til ulovlige formål.

Spyware

Spyware er programmer, som indsamler dine personlige oplysninger.

Spyware kan indsamle personlige oplysninger, herunder:

- internetsteder, du har gennemset
- e-mail-adresser fra computeren
- adgangskoder, eller
- kreditkortnumre.

Spyware installerer næsten altid sig selv uden udtrykkelig tilladelse. Spyware kan blive installeret sammen med et nyttigt program eller ved at narre dig til at klikke på en indstilling i et vildledende pop op-vindue.

Rootkits

Rootkits er programmer, der gør det vanskeligt at finde anden *malware*.

Rootkits gemmer filer og processer. Generelt gør de det for at skjule ondsindet aktivitet på din computer. Når en rootkit skjuler *malware*, er det ikke nemt at opdage, at din computer har malware.

Dette produkt har en rootkit-scanner, der specifikt scanner for rootkits, så *malware* ikke nemt kan skjules.

Riskware

Riskware er ikke beregnet specifikt til at skade computeren, men det kan skade computeren, hvis det misbruges.

Riskware er strengt taget ikke malware. Riskwareprogrammer udfører nogle nyttige, men potentielt farlige funktioner.

Eksempler på riskwareprogrammer er:

- programmer til onlinebeskeder (som IRC, Internet relay chat),
- programmer, der overfører filer via internettet fra en computer til en anden,
- internettelefonprogrammer (VoIP, *Voice over Internet Protocol*),
- software til fjernadgang, f.eks. VNC,
- scareware, som kan forsøge at skræmme eller lokke folk til at købe falske sikkerhedsprogrammer, eller
- software, der er udviklet til at omgå cd-kontroller eller kopibeskyttelse.

Hvis du udtrykkeligt har installeret programmet og konfigureret det korrekt, er det mindre sandsynligt, at det er skadeligt.

Hvis der er installeret riskware uden din viden, er det højst sandsynligt installeret med ondsindet hensigt og bør slettes.

Kapitel

4

Beskyttelse af computeren mod malware

Emner:

- *Sådan scannes min computer*
- *Sådan udelades filer fra scanningen*
- *Sådan anvendes karantæne*
- *Hvad er DeepGuard?*

Virus- og spywarescanning beskytter computeren mod programmer, som kan stjæle personlige oplysninger, beskadige computeren eller bruge den til ulovlige formål.

Som standard håndteres alle malwaretyper øjeblikkeligt, når de bliver fundet, så de ikke kan gøre nogen skade.

Virus- og spywarescanning scanner som standard dine lokale harddiske, flytbare medier (f.eks. bærbare drev eller cd'er) og overført indhold automatisk. Du kan også indstille den til at scanne din e-mails automatisk.

Virus- og spywarescanning overvåger også din computer for ændringer, der kan være et tegn på *malware*. Hvis der bliver fundet farlige systemændringer, f.eks. systemindstillinger eller forsøg på at ændre vigtige systemprocesser, forhindrer DeepGuard dette program i at køre, da det sandsynligvis er *malware*.

Sådan scannes min computer

Når Virus- og spywarescanning er slået til, scannes din computer automatisk for skadelige filer. Du kan også scanne filer manuelt og oprette planlagte scanninger.

Det anbefales, at Virus- og spywarescanning altid er slået til. Scan dine filer manuelt, når du vil sikre, at der ikke er skadelige filer på computeren, eller hvis du vil scanne filer, du har udeladt fra realtidsscanningen.

Ved at oprette en planlagt scanning fjerner Virus- og spywarescanning skadelige filer fra computeren på de angivne tidspunkter.

Scanne filer automatisk

Realtidsscanning beskytter din computer ved at scanne alle filer, når de håndteres, og ved at blokere adgangen til de filer, der indeholder *malware*.

Når din computer forsøger at få adgang til en fil, scanner Realtidsscanning filen for malware, før din computer får lov til at få adgang til den. Hvis Realtidsscanning finder skadeligt indhold, sætter den filen i karantæne, før den kan forårsage skade.

Påvirker realtidsscanningen min computers ydelse?

Normalt lægger du ikke mærke til scanningsprocessen, fordi den er hurtig og ikke kræver mange systemressourcer. Den mængde tid og Den mængde tid og de systemressourcer, som realtidsscanning kræver, afhænger f.eks. af filens indhold, placering og type.

Filer, som det tager længere tid at scanne:

- Filer på flytbare drev såsom cd'er, dvd'er og andre bærbare USB-drev.
- Komprimerede filer såsom *.zip*-filer.

  Bemærk: Komprimerede filer scannes som standard ikke.

Realtidsscanning kan gøre computeren langsommere, hvis:

- du har en computer, som ikke opfylder systemkravene, eller
- du åbner en masse filer samtidig. Eksempelvis når du åbner en mappe, som indeholder mange filer, der skal scannes.

Slå realtidsscanning til eller fra

Lad realtidsscanning være aktiveret for at standse *malware*, før det kan skade din computer.

Sådan slås realtidsscanning til eller fra:

1. På hovedsiden skal du klikke på **Status**.
2. Klik på **Skift indstillinger på denne side**.

   Bemærk: Du skal have administratorrettigheder til at deaktivere sikkerhedsfunktioner.

3. Slå **Virus- og spywarescanning** til eller fra.
4. Klik på **Luk**.

Håndtere skadelige filer automatisk

Realtidsscanning kan håndtere skadelige filer automatisk uden at stille dig spørgsmål.

Sådan lader du realtidsscanning håndtere skadelige filer automatisk:

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Computersikkerhed** > **Virus- og spywarescanning**.
3. Vælg **Håndter skadelige filer automatisk**.

Hvis du vælger ikke at håndtere skadelige filer automatisk, spørger realtidsscanning, hvad du vil gøre med en skadelig fil, når den bliver fundet.

Håndtere spyware

Virus- og spywarescanning blokerer spyware i det øjeblik, den forsøger at starte.

Inden et spywareprogram kan starte, blokerer produktet det og giver dig mulighed for at bestemme, hvad du vil gøre med det.

Vælg en af følgende handlinger, når der bliver fundet spyware:

Handl., der skal udføres	Hvad sker der med spywaren
Håndter automatisk	Lad produktet bestemme den bedste handling ud fra den spyware, der blev fundet.
Sæt spywaren i karantæne	Flyt spywaren til karantænen, hvor den ikke kan skade din computer.
Slet spywaren	Fjern alle spywarerelaterede filer fra computeren.
Bloker kun spywaren	Bloker adgang til spywaren, men lad den være på computeren.
Udelad spywaren fra scanningen	Tillad, at spywaren kører, og udelad den fra scanningen i fremtiden.

Håndtere riskware

Virus- og spywarescanning blokerer riskware i det øjeblik, den forsøger at starte.

Inden et riskwareprogram kan starte, blokerer produktet det og giver dig mulighed for at bestemme, hvad du vil gøre med det.

Vælg en af følgende handlinger, når der bliver fundet riskware:

Handl., der skal udføres	Hvad sker der med riskware
Bloker kun riskwaren	Bloker adgang til riskwaren, men lad den være på computeren.
Sæt riskwaren i karantæne	Flyt riskwaren til karantænen, hvor den ikke kan skade din computer.
Slet riskwaren	Flern alle riskwarerelaterede filer fra computeren.
Udelad riskwaren fra scanningen	Tillad, at riskwaren kører, og udelad den fra scanningen i fremtiden.

Fjerne tracking cookies automatisk

Ved at fjerne tracking cookies forhindrer du websteder i at kunne spore det websteder, du besøger på internettet.

Tracking cookies er små filer, som gør websteder i stand til at registrere, hvilke websteder du besøger. Følg disse anvisninger for at holde tracking cookies væk fra computeren.

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Computersikkerhed** > **Virus- og spywarescanning**.
3. Vælg **Fjern tracking cookies**.
4. Klik på **OK**.

Scanne filer manuelt

Du kan scanne dine filer manuelt, eksempelvis når du tilslutter en ekstern enhed til computeren, for at sikre, at den ikke indeholder malware.

Starte den manuelle scanning

Du kan scanne hele computeren eller scanne for en specifik type *malware* eller et specifikt sted.

Hvis du har mistanke om en bestemt type *malware*, kan du scanne udelukkende for denne type. Hvis du har mistanke om malware på et bestemt sted på computeren, kan du foretage scanning alene på det sted. Disse scanninger afsluttes meget hurtigere end scanning af hele computeren.

For at starte manuel scanning på din computer:

1. Klik på pilen under **Scan** på hovedsiden.

   Scanningsindstillingerne vises.
2. Vælg scanningstype.

   Vælg **Skift scanningsindstillinger** for at optimere, hvordan den manuelle scanning scanner computeren for virus og andre skadelige programmer.
3. Hvis du valgte **Vælg, hvad der skal scannes**, åbnes et vindue, hvor du kan vælge, hvilken placering du vil scanne.
   Scanningsguide åbnes.

Scanningstyper

Du kan scanne hele computeren eller scanne for en specifik type malware eller et specifikt sted.

I det følgende er der en oversigt over forskellige scanningstyper:

Scanningstype	Hvad der scannes	Hvornår denne type bruges
Virus- og spywarescanning	Dele af computeren for virus, spyware og riskware	Denne scanningstype er meget hurtige end en fuld scanning. Den søger kun på de dele af computeren, som indeholder installerede programfiler. Denne scanningstype anbefales, hvis du ønsker en hurtig kontrol af, om computeren er ren, fordi den kan finde og fjerne eventuel aktiv malware på computeren på en effektiv måde.
Fuld computerscanning	Hele computeren (interne og eksterne harddiske) for virus, spyware og riskware	Når du vil være helt sikker på, at der ikke er malware eller riskware på din computer.Denne scanningstype tager længst tid at fuldføre. Den kombinerer en hurtig scanning for malware og en harddiskscanning. Den kontrollerer også, om der er elementer, som kan være skjult af et rootkit.
Vælg, hvad der skal scannes	En bestemt fil, mappe eller disk for virus, spyware og riskware	Hvis du har mistanke om, at et bestemt sted på din computer kan have malware. Det kan f.eks. være, at der på stedet er overførsler fra potentielt farlige kilder såsom peer to peer-fildelingsnetværk. Den tid, scanningen tager, afhænger af størrelsen på den destination, du scanner. Scanningen er hurtig færdig, hvis du f.eks. scanner en mappe, der kun indeholder nogle få små filer.

Scanningstype	Hvad der scannes	Hvornår denne type bruges
Rootkit-scanning	Vigtige systemsteder, hvor et mistænkeligt element kan betyde et sikkerhedsproblem. Scanner for skjulte filer, mapper, diske eller processer	Når du forventer, at et rootkit kan være installeret på computeren. Eksempelvis hvis malware for nylig blev registreret på computeren, og du gerne vil være sikker på, at det ikke installerede et rootkit.

Scanne i Windows Stifinder

Du kan scanne diske, mapper og filer for *virus*, *spyware* og *riskware* i Windows Stifinder.

Sådan scannes en disk, mappe eller fil:

1. Placer din musemarkør på, og højreklik på den disk, mappe eller fil, du ønsker at scanne.
2. Fra genvejsmenuen skal du vælge **Scan mapper for at se, om der er viruser**. (Indstillingsnavnet afhænger af, om du scanner en disk, mappe eller fil.)
   Vinduet **Scanningsguide** åbner, og scanningen starter.

Hvis der blev fundet *virus* eller *spyware*, viser **Scanningsguide**n, hvordan du foretager en desinficering.

Vælge filer, der skal scannes

Vælg de filtyper, der skal scannes for *virus* og *spyware* i manuelle og planlagte scanninger.

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Andre indstillinger** > **Manuel scanning**.
3. Vælg mellem følgende indstillinger under **Scanningsindstillinger**:

   Scan kun kendte filtyper
   For kun at scanne de filtyper, hvor det er mest sandsynligt, at der kan være inficeringer, f.eks. eksekverbare filer. Scanningen er også hurtigere, når du vælger denne indstilling. Filerne med følgende filtyper scannes: `.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`.

   Scan i komprimerede filer
   For at scanne arkivfiler og mapper.

   Brug avanceret heuristik
   For at bruge den tilgængelige heuristik under scanningen for bedre at finde ny eller ukendt malware.

   Bemærk: Hvis du vælger denne indstilling, tager scanningen længere tid, og det kan medføre flere falske positiver (harmløse filer, der rapporteres som mistænkelige).

4. Klik på **OK**.

Bemærk: Udeladte filer på listen over udeladte elementer scannes ikke, selv hvis du vælger, at de skal scannes her.

Gør følgende, når der bliver fundet skadelige filer

Vælg, hvordan du vil håndtere skadelige filer, når de bliver fundet.

Sådan vælges den ønskede handling, når der bliver fundet skadeligt indhold under den manuelle scanning:

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Andre indstillinger** > **Manuel scanning**.
3. Vælg en af følgende indstillinger i **Når virus eller spyware bliver fundet**:

Indstilling	Beskrivelse
Spørg mig (standard)	Du kan vælge handlingen for hvert element, der bliver fundet under den manuelle scanning.
Rens filerne	Produktet forsøger automatisk at rense inficerede filer, der bliver fundet under den manuelle scanning. **Bemærk:** Hvis produktet ikke kan rense den inficerede fil, sættes den i karantæne (medmindre den bliver fundet på netværket eller flytbare drev), så den ikke kan skade computeren.
Sæt filerne i karantæne	Produktet flytter skadelige filer, der bliver fundet under den manuel scanning, til karantænen, hvor de ikke kan skade computeren.
Slet automatisk	Produktet sletter skadelige filer, der bliver fundet under den manuelle scanning.
Kun rapport	Produkter gør ikke noget ved skadelige filer, der bliver fundet under den manuelle scanning, og registrerer det i scanningsrapporten. **Bemærk:** Hvis realtidsscanning er slået fra, kan malware stadig skade computeren, hvis du vælger denne indstilling.

Bemærk: Når der bliver fundet skadelige filer under den planlagte scanning, renses de automatisk.

Planlæg en scanning

Indstil din computer til at scanne og fjerne virus og andre skadelige programmer automatisk, når du ikke bruger den, eller indstil scanningen til at køre regelmæssigt for at sikre, at din computer ikke er inficeret.

Sådan planlægges en scanning:

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Andre indstillinger** > **Planlagt scanning**.
3. Slå **Planlagt scanning** til.
4. Vælg, hvornår scanningen skal starte.

Indstilling	Beskrivelse
Dagligt	Scan computeren hver dag.
Ugentligt	Scan computeren på de valgte ugedage. Vælg dagene på listen.
Månedligt	Scan computeren på de valgte dage i måneden. Sådan vælges dagene: 1. Vælg en af indstillingerne for **Dag**.

Indstilling	Beskrivelse
	2. Vælg en dag i måneden fra listen ved siden af den valgte dag.

5. Vælg, hvordan du ønsker at starte scanningen på udvalgte dage.

Indstilling	Beskrivelse
Starttid	Start scanningen på det angivne tidspunkt.
Når computer ikke er brugt i	Start scanningen, når du ikke har brugt computeren i det angivne tidsrum.

Planlagt scanning bruger indstillingerne for manuel scanning, når computeren scannes, bortset fra at den scanner arkiver hver gang og automatisk renser computeren for skadelige filer.

Scanne e-mails

E-mail-scanning beskytter dig mod skadelige filer i e-mails, der sendes til dig.

Virus- og spywarescanning skal være aktiveret for at scanne e-mails for virus.

Sådan slås e-mail-scanning til:

1. Klik på Indstillinger på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg Computersikkerhed > Virus- og spywarescanning.
3. Vælg Fjern skadelige filer vedhæftet e-mail.
4. Klik på OK.

Hvornår e-mail-meddelelser og vedhæftede filer scannes

Virus- og spywarescanning kan fjerne skadeligt indholder fra e-mails, som du modtager.

Virus- og spywarescanning fjerner skadelige e-mails, der modtages af e-mail-programmer som f.eks. Microsoft Outlook og Outlook Express, Microsoft Mail eller Mozilla Thunderbird. Ikke-krypterede e-mails og vedhæftede filer scannes, hver gang e-mail-programmet modtager dem fra e-mail-serveren via POP3-protokollen.

Virus- og spywarescanning kan ikke scanne e-mails i webmail, som omfatter e-mail-programmer, der kører i webbrowseren som f.eks. Hotmail, Yahoo! mail eller Gmail. Du er stadig beskyttet mod *virus*, selvom du ikke fjerner skadelige vedhæftede filer, eller hvis du bruger webmail. Når du åbner vedhæftede filer, fjerner realtidsscanningen skadelige vedhæftede filer, før de kan forårsage skade.

Bemærk: Realtidsscanning beskytter kun din computer, men ikke dine venners. Realtidsscanning scanner ikke vedhæftede filer, medmindre du åbner den vedhæftede fil. Det betyder, at hvis du bruger webmail, og du videresender en meddelelse, inden du har åbnet den vedhæftede fil, kan du komme til at videresende en inficeret e-mail til dine venner.

Vise scanningsresultaterne

I virus- og spywareoversigten vises alle skadelige filer, som produktet har fundet.

Produktet kan sommetider ikke udføre den handling, du har valgt, når der bliver fundet noget skadeligt. Hvis du f.eks. vælger at rense filer, og en fil ikke kan renses, flyttes den til karantænen. Du kan få vist disse oplysninger i virus- og spywareoversigten.

Sådan vises oversigten:

1. Klik på Indstillinger på hovedsiden.

Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Computersikkerhed** > **Virus- og spywarescanning**.
3. Klik på **Vis fjernelsesoversigt**.

Følgende oplysninger vises i virus- og spywareoversigten:

- dato og klokkeslæt, da den skadelige fil blev fundet,
- navnet på malwaren og placeringen på din computer og
- den udførte handling.

Sådan udelades filer fra scanningen

Du kan nogle gange have behov for at udelade nogle filer eller programmer fra scanningen. Udeladte elementer scannes ikke, medmindre du fjerner dem fra listen over udeladte elementer.

Bemærk: Der er særskilte udeladelseslister til realtidsscanning og manuel scanning. Hvis du f.eks. vil udelade en fil fra realtidsscanningen, scannes den under den manuelle scanning, medmindre du også udelader den fra den manuelle scanning.

Udelad filtyper

Når du udelader filer efter filtype, scannes filer med de angivne filtyper ikke for skadeligt indhold.

Sådan tilføjes eller fjernes en filtype, du vil udelade:

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg, om du vil udelade filtypen fra realtidsscanning eller manuel scanning:
   - Vælg **Computersikkerhed** > **Virus- og spywarescanning** for at udelade filtypen fra realtidsscanning.
   - Vælg **Andre indstillinger** > **Manuel scanning** for at udelade filtypen fra manuel scanning.
3. Klik på **Udelad filer fra scanningen**.
4. Sådan udelades en filtype:
   a) Vælg fanen **Filtyper**.
   b) Vælg **Udelad filer med disse filtyper**.
   c) Indtast en filtype, som angiver, hvilke typer filer du vil udelade, i feltet ved siden af knappen **Tilføj**.

      Hvis du vil angive filer, der ikke har nogen filtype, skal du indtaste '.'. Du kan bruge jokertegnet '?' til at angive et vilkårligt tegn eller '*' til at angive et hvilket som helst antal tegn.

      Hvis du f.eks. vil udelade eksekverbare filer, skal du indtaste `exe` i feltet.
   d) Klik på **Tilføj**.
5. Gentag det forrige trin for en hvilken som helst anden filtype, der skal udelades fra at blive scannet for virus.
6. Klik på **OK** for at lukke dialogboksen **Udelad fra scanning**.
7. Klik på **OK** for at anvende de nye indstillinger.

De valgte filtyper udelades fra fremtidige scanninger.

Udelad filer efter placering

Når du udelader filer efter placering, scannes filer på de angivne drev eller mapper ikke for skadeligt indhold.

Sådan tilføjes eller fjernes filplaceringer, som du vil udelade:

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg, om du vil udelade placeringen fra realtidsscanning eller manuel scanning:
   - Vælg **Computer** > **Virus- og spywarescanning** for at udelade placeringen fra realtidsscanning.
   - Vælg **Computer** > **Manuel scanning** for at udelade placeringen fra manuel scanning.
3. Klik på **Udelad filer fra scanningen**.
4. Sådan udelades en fil, disk eller mappe:
   a) Vælg fanen **Objekter**.
   b) Vælg **Udelad objekter (filer, mapper, ...)**.
   c) Klik på **Tilføj**.
   d) Vælg den fil, det drev eller den mappe, som du vil udelade fra virus- scanning.

      Bemærk: Nogle drev kan muligvis fjernes, som cd-, dvd- eller netværksdrev. Neværksdrev og tomme drev, der kan fjernes kan ikke udelades.

   e) Klik på **OK**.
5. Gentag foregående trin for at undlade andre filer, drev eller mapper fra at blive virusscannet.
6. Klik på **OK** for at lukke **Udelad fra scanning**.
7. Klik på **OK** for at de nye indstillinger træder i kraft.

De valgte filer, drev eller mapper udelades fra fremtidige scanninger.

Vis udeladte programmer

Du kan få vist programmer, som du har udeladt fra scanningen, og fjerne dem fra listen over udeladte elementer, hvis du vil scanne dem fremover.

Hvis realtidsscanningen eller den manuelle scanning registrerer et program, der opfører sig som spyware eller riskware, men du ved, at det er sikkert, kan du udelade det fra scanningen, så produktet ikke længere advarer dig om det.

Bemærk: Hvis programmet opfører sig som en virus eller andet ondsindet program, kan det ikke udelades.

Du kan ikke udelade programmer direkte. Nye programmer vises kun på udeladelseslisten, hvis du udelader dem under scanningen.

Sådan vises de programmer, der er udeladt fra scanningen:

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg, om du vil se programmer, der er udeladt fra realtidsscanning eller manuel scanning:
   - Vælg **Computer** > **Virus- og spywarescanning** for at se programmer, der er udeladt fra realtidsscanning.
   - Vælg **Computer** > **Manuel scanning** for at se programmer, der er udeladt fra manuel scanning.
3. Klik på **Udelad filer fra scanningen**.
4. Vælg fanen **Programmer**.

   Bemærk: Det er kun spyware - og riskwareprogrammer, der kan udelades, ikke virus.

5. Hvis du igen vil scanne det udeladte program:
   a) Vælg det program, du vil medtage i scanningen.
   b) Klik på **Fjern**.
6. Klik på **OK** for at lukke dialogboksen **Udelad fra scanning**.
7. Klik på **OK** for at afslutte.

Sådan anvendes karantæne

Karantæne er et sikkert lager for filer, der kan være skadelige.

Filer i karantæne kan ikke spredes og forårsager ingen skade på din computer.

Du kan sætte *malware*, *spyware* og *riskware* i karantæne for at gøre dem harmløse. Du kan gendanne programmer eller filer fra karantæne senere, hvis du har brug for dem.

Hvis du ikke har brug for et element i karantæne, kan du slette det. Ved at slette elementet i karantæne fjernes det permanent fra din computer.

- Generelt kan du slette *malware* i karantæne.
- I de fleste tilfælde kan du slette *spyware* i karantæne. Det er muligt, at *spyware* i karantæne er en del af det lovlige softwareprogram, og at du ved at fjerne den forhindrer det pågældende program i at fungere korrekt. Hvis du vil bevare programmet på din computer, kan du gendanne *spyware* i karantæne.
- *Riskware* i karantæne kan være et lovligt softwareprogram. Hvis du selv har installeret og konfigureret programmet, kan du gendanne det fra karantæne. Hvis *riskware* er installeret uden din viden, er det højst sandsynligt installeret med ondsindet hensigt og bør slettes.

Vis elementer i karantæne

Få vist flere oplysninger om elementer i karantæne.

For at få vist detaljerede oplysninger om elementer i karantæne:

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Computersikkerhed** > **Virus- og spywarescanning**.
3. Klik på **Vis karantæne**.
   På siden **Karantæne** vises det samlede antal elementer, der er gemt i karantænen.
4. Du kan få vist detaljerede oplysninger om elementerne i karantænen ved at klikke på **Detaljer**.

   Du kan sortere indholdet efter malwarenavn eller filsti.

   Der vises en liste over de første 100 elementer i karantænen med deres type, navn og den sti, hvor filerne blev installeret.
5. Hvis du vil have vist flere oplysninger om et element i karantænen, skal du klikke på ikonet ud for elementet i kolonnen **Tilstand**.

Gendan elementer i karantæne

Du kan gendanne de elementer i karantæne, som du har brug for.

Du kan gendanne programmer eller filer fra karantæne, hvis du har brug for dem. Du skal ikke gendanne elementer fra karantæne, medmindre du er sikker på, elementerne ikke udgør en trussel. Gendannede elementer placeres på deres oprindelige plads på din computer.

Gendan elementer i karantæne

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Computersikkerhed** > **Virus- og spywarescanning**.
3. Vis på **Vis karantæne**.
4. Marker de elementer i karantænen, der skal gendannes.
5. Klik på **Gendan**.

Hvad er DeepGuard?

DeepGuard analyserer indholdet af filer og programmers adfærd samt overvåger programmer, der ikke er tillid til.

DeepGuard blokerer nye og ikke-opdagede *virus*, *orme* og andre skadelige programmer, der forsøger at foretage ændringer af din computer, og forhindrer mistænkelige programmer i at få adgang til internettet.

Når DeepGuard registrerer et nyt program, der forsøger at foretage potentielt skadelige ændringer af systemet, tillader det programmet at køre i en sikker zone. I den sikre zone kan programmet ikke skade din computer. DeepGuard analyserer, hvilke ændringer programmet forsøgte at foretage, og beslutter baseret på dette, hvor sandsynligt det er, at programmet er *malware*. Hvis det er sandsynligt, at programmet er *malware*, blokerer DeepGuard for det.

Potentielt skadelige systemændringer, som DeepGuard registrerer, omfatter:

- ændringer af systemindstillinger (Windows registreringsdatabase),
- forsøg på at slå vigtige systemer fra, f.eks. sikkerhedsprogrammer som dette produkt, og
- forsøg på at redigere vigtige systemfiler.

Slå DeepGuard til eller fra

Lad DeepGuard være aktiveret for at forhindre mistænkelige programmer i at foretage potentielt skadelige systemændringer på din computer.

Hvis du har Windows XP, skal du sørge for at installere Service Pack 2, før du slår DeepGuard til.

Sådan slås DeepGuard til eller fra:

1. På hovedsiden skal du klikke på **Status**.
2. Klik på **Skift indstillinger på denne side**.

   Bemærk: Du skal have administratorrettigheder til at deaktivere sikkerhedsfunktioner.

3. Slå **DeepGuard** til eller fra.
4. Klik på **Luk**.

Tillade programmer, som DeepGuard har blokeret

Du kan styre, hvilke programmer DeepGuard tillader og blokerer.

DeepGuard kan sommetider forhindre et sikkert program i at køre, selvom du vil bruge programmet og ved, at det er sikkert. Det sker, fordi programmet forsøger at foretage systemændringer, der kan være skadelige. Du kan også utilsigtet have blokeret programmet, da der blev vist en pop op-meddelelse fra DeepGuard.

Sådan tillades det program, som DeepGuard har blokeret:

1. Klik på **Værktøjer** på hovedsiden.
2. Klik på **Programmer**.
   Listen **Overvågede programmer** vises.
3. Find det program, du vil tillade.

   Bemærk: Du kan klikke på kolonneoverskrifterne for at sortere listen. Klik f.eks. på kolonnen **Tilladelse** for at sortere listen i grupper med tilladte og afviste programmer.

4. Vælg **Tillad** i kolonnen **Tilladelse**.
5. Klik på **Luk**.

DeepGuard tillader, at programmet foretager systemændringer igen.

Bruge DeepGuard i kompatibilitetstilstand

Af hensyn til maksimal beskyttelse ændrer DeepGuard midlertidigt programmer, der kører. Nogle programmer kontrollerer, at de ikke ødelægges eller ændres og er muligvis ikke kompatible med denne funktion. Eksempelvis kontrollerer onlinespil med værktøjer mod snyderi, at de ikke er blevet ændret på nogen måde, når de køres. I disse tilfælde kan du aktivere kompatibilitetstilstanden.

Sådan aktiveres kompatibilitetstilstanden:

1. Klik på **Indstillinger** på hovedsiden.

   Bemærk: Du skal have administratorrettigheder for at ændre indstillingerne.

2. Vælg **Computersikkerhed** > **DeepGuard**.
3. Vælg **Brug kompatibilitetstilstanden**.
4. Klik på **OK**.

Gør følgende med advarsler om mistænkelig adfærd

DeepGuard overvåger programmer, der ikke er tillid til. Hvis et overvåget program forsøger at få adgang til internettet, forsøger at foretage ændringer af systemet eller opfører sig mistænkeligt, blokeres det af DeepGuard.

Når du har valgt **Advar mig om mistænkelig adfærd** i DeepGuard-indstillingerne, giver DeepGuard dig besked, når der registreres et potentielt skadeligt program, eller når du starter et program med et ukendt omdømme.

Sådan bestemmer du, hvad du vil gøre med et program, som DeepGuard har blokeret:

1. Klik på **Detaljer** for at se flere oplysninger om programmet.
   I afsnittet med detaljer kan du se:
   - programmets placering,
   - programmets omdømme i realtidsbeskyttelsesnetværket, og
   - hvor almindeligt programmet er.
2. Bestem, om du har tillid til det program, som DeepGuard har blokeret:
   - Vælg **Jeg har tillid til programmet. Lad det fortsætte.**, hvis du ikke vil blokere programmet.

     Det er mere sandsynligt, at programmet er sikkert, hvis:

     - DeepGuard blokerede program som følge af noget, du gjorde,
     - du genkender programmet, eller
     - du fik programmet fra en pålidelig kilde.

- Vælg **Jeg har ikke tillid til programmet. Hold det blokeret.**, hvis programmet fortsat skal være blokeret.

  Det er mere sandsynligt, at programmet er usikkert, hvis:

  - programmet ikke er almindeligt,
  - programmet har et ukendt omdømme, eller
  - du ikke kender programmet.

3. Hvis du vil indsende et mistænkeligt program til analyse:

a) Klik på **Rapporter programmet til F-Secure**.
Produktet viser betingelserne for indsendelse.

b) Klik på **Accepter**, hvis du accepterer betingelserne og vil indsende prøven.

Det anbefales, at du sender en prøve, når:

- DeepGuard blokerer et program, og du ved, at det er sikkert, eller
- du har mistanke om, at programmet kan være *malware*.