F-Secure Anti-Virus 2013

Cuprins

Capitolul 1: Instalare.....5

Înainte de instalarea pentru prima dată.....6
Instalarea pentru prima dată a produsului.....6
Instalarea şi upgrade-ul aplicațiilor.....6
Ajutor şi asistență.....7

Capitolul 2: Introducere.....9

Cum puteți utiliza actualizările automate.....10
Verificarea stării de actualizare.....10
Modificarea setărilor conexiunii la Internet.....10
Verificarea stării pentru Rețeaua de protecție în timp real.....11
Cum puteți vedea ce a efectuat produsul.....11
Vizualizarea istoricului notificărilor.....11
Modificarea setărilor pentru notificări.....11
Rețeaua de protecție în timp real.....12
Ce este Rețeaua de protecție în timp real.....12
Avantajele oferite de Rețeaua de protecție în timp real.....12
Cu ce date contribuiți.....13
Cum vă protejăm confidențialitatea.....14
Cum deveniți colaborator la Rețeaua de protecție în timp real.....14
Întrebări despre rețeaua de protecție în timp real.....15
Cum ştiu dacă abonamentul meu este valid.....15
Centrul de acțiuni.....15
Activarea abonamentului.....16

Capitolul 3: Introducere.....17

Vizualizarea stării generale a protecției mele.....18
Vizualizați statisticile produsului.....18
Gestionarea actualizărilor produsului.....19
Vizualizarea versiunii bazei de date.....19
Modificarea setărilor pentru rețeaua de bandă largă mobilă.....19
Ce reprezintă viruşii şi alte programe malware.....20
Viruşi.....20
Spyware.....21
Programe rootkit.....21
Riskware.....21

Capitolul 4: Protejarea computerului împotriva programelor malware.23
Cum pot scana computerul meu....24
Scanați fişierele în mod automat....24
Scanați manual fişierele....26
Scanarea e-mailurilor....29
Vizualizarea rezultatelor scanării....30
Cum excludeți fişiere din scanare....30
Excluderea tipurilor de fişiere....30
Excluderea fişierelor după locație....31
Vizualizarea aplicațiilor excluse....31
Cum puteți utiliza carantina....32
Vizualizare elemente din carantină....33
Restabilirea elementelor din carantină....33
Ce reprezintă DeepGuard....33
Activați şi dezactivați DeepGuard....34
Permiteți executarea aplicațiilor pe care DeepGuard le-a blocat....34
Utilizarea DeepGuard în modul de compatibilitate....34
Ce este de făcut în cazul avertismentelor de comportament suspect....35

Capitolul

1

Instalare

Subiecte:

- *Înainte de instalarea pentru prima dată*
- *Instalarea pentru prima dată a produsului*
- *Instalarea şi upgrade-ul aplicațiilor*
- *Ajutor şi asistență*

Înainte de instalarea pentru prima dată

Vă mulțumim că ați ales F-Secure.

Pentru a instala produsul, aveți nevoie de următoarele:

- CD-ul de instalare sau un pachet de instalare. Dacă utilizați un netbook fără o unitate pentru CD, puteți descărca pachetul de instalare de la adresa *www.f-secure.com/netbook*.
- Cheia dvs. de abonament.
- O conexiune Internet.

Dacă aveți un produs de securitate de la alt producător, programul de instalare va încerca să îl elimine automat. Dacă nu se întâmplă acest lucru, eliminați-l manual.

Notă: Dacă aveți mai multe conturi pe computer, conectați-vă cu privilegii de administrator la instalare.

Instalarea pentru prima dată a produsului

Instrucțiuni de instalare a produsului.

Urmați aceste instrucțiuni pentru a instala produsul:

1. Introduceți CD-ul sau faceți dublu clic pe programul de instalare pe care l-ați descărcat.

   Dacă CD-ul nu porneşte automat, accesați Windows Explorer, faceți dublu clic pe pictograma CD-ROM şi faceți dublu clic pe fişierul de instalare pentru a începe instalarea.

2. Urmați instrucțiunile de pe ecran.

   - Dacă ați achiziționat produsul pe un CD de la un magazin, puteți găsi cheia de abonament pe coperta Ghidului de instalare rapidă.
   - Dacă ați descărcat produsul de pe F-Secure eStore, cheia de abonament este inclusă în e-mailul de confirmare a comenzii de achiziționare.

   Este posibil să fie necesară repornirea computerului înainte de a valida abonamentul şi de a descărca cele mai recente actualizări de pe Internet. Dacă instalați de pe CD, rețineți că trebuie să scoateți CD-ul de instalare înainte de a reporni computerul.

Instalarea şi upgrade-ul aplicațiilor

Instrucțiuni pentru activarea noului abonament.

Urmați aceste instrucțiuni pentru a activa noul abonament sau pentru a instala o nouă aplicație utilizând panoul de lansare:

Notă: Puteți găsi pictograma panoului de lansare în bara de sistem Windows.

1. Pe panoul de lansare, faceți clic dreapta pe pictograma din extrema dreaptă.
   Se deschide un meniu de tip pop-up.
2. Selectați **Vizualizare abonamentele mele**
3. În **Abonamentele mele**, accesați pagina **Stare abonament**, apoi faceți clic pe **Activare abonament**.
   Se deschide fereastra **Activare abonament**.
4. Introduceți cheia de abonament pentru aplicație, apoi faceți clic pe **OK**.

5. După validarea şi activarea abonamentului, faceți clic pe **Închidere**.
6. În **Abonamentele mele**, accesați pagina **Stare instalare**. Dacă instalarea nu porneşte automat, urmați aceste instrucțiuni:
   a) Faceți clic pe **Instalare**.
      Se deschide fereastra de instalare.
   b) Faceți clic pe **Următorul**.
      Aplicația este descărcată, iar instalarea porneşte.
   c) La finalizarea instalării, faceți clic pe **Închidere**.

Noul abonament a fost activat.

Ajutor şi asistență

Puteți accesa online ajutorul pentru produs făcând clic pe pictograma Ajutor sau apăsând pe `F1` în orice ecran al produsului.

După ce înregistrați licența, aveți dreptul la servicii suplimentare, cum ar fi actualizări gratuite ale produsului şi asistență pentru produs. Puteți înregistra la adresa *www.f-secure.com/register*.

Capitolul

2

Introducere

Subiecte:

- *Cum puteți utiliza actualizările automate*
- *Cum puteți vedea ce a efectuat produsul*
- *Rețeaua de protecție în timp real*
- *Cum ştiu dacă abonamentul meu este valid*

Informații privind modul în care începeți să utilizați produsul.

Această secțiune descrie modul în care se modifică setările comune şi se gestionează abonamentele dvs. prin panoul de lansare.

Setările comune ale panoului de lansare sunt setări care se aplică tuturor programelor instalate pe panoul de lansare. În loc să schimbați setările separat pentru fiecare program, puteți edita setările comune, care vor fi utilizate ulterior de toate programele instalate.

Setările comune ale panoului de lansare includ:

- Descărcări, unde puteți să vedeți informații despre actualizările descărcate şi puteți să verificați manual dacă sunt disponibile actualizări noi.
- Setări conexiune, unde puteți modifica modul în care computerul se conectează la Internet.
- Notificări, unde puteți vizualiza notificările anterioare şi puteți seta ce tip de notificări doriți să vedeți.
- Setări confidențialitate, unde puteți să selectați dacă permiteți computerului să se conecteze la Rețeaua de protecție în timp real.

De asemenea, puteți gestiona abonamentele pentru programele instalate prin panoul de control.

Cum puteți utiliza actualizările automate

Actualizările automate mențin protecția computerului dvs. actualizată.

Produsul preia cele mai recente actualizări pe computerul dvs. când sunteți conectat la Internet. Detectează traficul de rețea şi nu deranjează alte utilizări ale Internetului, chiar şi cu o conexiune slabă de rețea.

Verificarea stării de actualizare

Vizualizați data şi ora celei mai recente actualizări.

Dacă actualizările automate sunt activate, produsul primeşte automat cele mai recente actualizări când sunteți conectat la Internet.

Pentru a vă asigura că aveți cele mai recente actualizări:

1. Pe panoul de lansare, faceți clic dreapta pe pictograma din extrema dreaptă.
   Va apărea un meniu de tip pop-up.
2. Selectați **Deschidere setări comune**.
3. Selectați **Actualizări automate** > **Descărcări**.
4. Faceți clic pe **Verificare imediată**.
   Produsul se conectează la Internet şi caută cele mai recente actualizări. Dacă protecția nu este actualizată, acesta va prelua cele mai recente actualizări.

   Notă: Dacă utilizați un modem sau dacă aveți o conexiune ISDN la Internet, conexiunea trebuie să fie activă pentru a verifica actualizările.

Modificarea setărilor conexiunii la Internet

În mod obişnuit nu este necesar să modificați setările standard, dar puteți configura modul în care este conectat serverul la Internet, aşa încât să puteți primi actualizările în mod automat.

Pentru a modifica setările conexiunii la Internet:

1. Pe panoul de lansare, faceți clic dreapta pe pictograma din extrema dreaptă.
   Va apărea un meniu de tip pop-up.
2. Selectați **Deschidere setări comune**.
3. Selectați **Actualizări automate** > **Conexiune**.
4. Din lista **Conexiune Internet**, selectați modul în care computerul este conectat la Internet.
   - Selectați **Se presupune conectat întotdeauna** dacă aveți o conectare permanentă la rețea.

     Notă: În cazul în care computerul nu are o conexiune permanentă la rețea, ci este configurat pentru apelare-la-cerere, selectarea opțiunii **Se presupune conectat întotdeauna** poate avea ca rezultat mai multe apelări.
   - Selectați **Detectare conexiune** pentru a prelua actualizări numai atunci când produsul detectează o conexiune activă la rețea.
   - Selectați **Detectare trafic** pentru a prelua actualizări numai atunci când produsul detectează alt trafic de rețea.

     Sfat: Dacă aveți o configurație neobişnuită care face ca setarea **Detectare conexiune** să detecteze o conexiune activă la rețea, chiar dacă nu există nicio conexiune, selectați **Detectare trafic** în schimb.

5. În lista **Proxy HTTP**, selectați dacă acest computer utilizează sau nu un *server proxy* pentru a se conecta la Internet.
   - Selectați **Niciun proxy HTTP** în cazul în care computerul este conectat direct la Internet.
   - Selectați **Configurare manuală proxy HTTP** pentru a configura setările *Proxy HTTP*.
   - Selectați **Utilizare proxy HTTP al browserului meu**pentru a utiliza aceleaşi setări *Proxy HTTP* pe care le-ați configurat în browserul Web.

Verificarea stării pentru Rețeaua de protecție în timp real

Pentru a funcționa corect, multe dintre caracteristicile produsului depind de conectivitatea Rețelei de protecție în timp real.

Dacă există probleme în rețea sau dacă firewallul blochează traficul Rețelei de protecție în timp real, starea este „deconectată”. Dacă nu sunt instalate funcții ale produsului care să necesite accesul la Rețeaua de protecție în timp real, starea este „în aşteptare”.

Pentru a verifica starea:

1. Pe panoul de lansare, faceți clic dreapta pe pictograma din extrema dreaptă.
   Va apărea un meniu de tip pop-up.
2. Selectați **Deschidere setări comune**.
3. Selectați **Actualizări automate** > **Conexiune**.

Sub **Rețea de protecție în timp real** puteți verifica starea curentă a acesteia.

Cum puteți vedea ce a efectuat produsul

Puteți să vedeți acțiunile efectuate de produs pentru a vă proteja computerul în pagina **Notificări**.

Produsul va afişa o notificare dacă efectuează o acțiune, de exemplu, dacă găseşte un virus pe care îl blochează. Unele notificări pot fi trimise şi de furnizorul de servicii, de exemplu, pentru a vă înştiința despre noile servicii disponibile.

Vizualizarea istoricului notificărilor

Puteți să vedeți ce notificări au fost afişate în istoricul de notificări

Pentru a vizualiza istoricul de notificări:

1. Pe panoul de lansare, faceți clic dreapta pe pictograma din extrema dreaptă.
   Va apărea un meniu de tip pop-up.
2. Selectați **Deschidere setări comune**.
3. Selectați **Altele** > **Notificări**.
4. Faceți clic pe **Afişare istoric notificări**.
   Se deschide lista cu istoricul de notificări.

Modificarea setărilor pentru notificări

Puteți selecta tipul notificărilor pe care doriți ca produsul să le afişeze.

Pentru a modifica setările pentru notificări:

1. Pe panoul de lansare, faceți clic dreapta pe pictograma din extrema dreaptă.
   Va apărea un meniu de tip pop-up.

2. Selectați **Deschidere setări comune**.
3. Selectați **Altele** > **Notificări**.
4. Selectați sau debifați **Se permit mesaje pentru programe** pentru a activa sau a dezactiva mesajele pentru programe.

   Când această setare este activată, produsul va afişa notificări de la programele instalate.
5. Selectați sau debifați **Se permit mesaje promoționale** pentru a activa sau a dezactiva mesajele promoționale.
6. Faceți clic pe **OK**.

Rețeaua de protecție în timp real

Acest document descrie Rețeaua de protecție în timp real, un serviciu online oferit de F-Secure Corporation, serviciu care identifică aplicațiile şi site-urile Web curate, oferind în acelaşi timp protecție împotriva programelor malware şi a programelor exploit de pe site-urile Web.

Ce este Rețeaua de protecție în timp real

Rețeaua de protecție în timp real este un serviciu online care oferă un răspuns rapid împotriva celor mai recente amenințări de pe Internet.

În calitate de colaborator la Rețeaua de protecție în timp real, puteți să ne ajutați să întărim protecția împotriva amenințărilor noi şi în continuă dezvoltare. Rețeaua de protecție în timp real colectează statistici ale anumitor aplicații necunoscute, rău intenționate sau suspecte şi despre ceea ce fac acestea pe dispozitivul dvs. Aceste informații sunt anonime şi sunt trimise la F-Secure Corporation pentru o analiză combinată a datelor. Utilizăm informațiile analizate pentru a îmbunătăți securitatea pe dispozitivul dvs. împotriva celor mai recente amenințări şi a fişierelor rău intenționate.

Cum funcționează Rețeaua de protecție în timp real

În calitate de colaborator la Rețeaua de protecție în timp real, puteți oferi informații despre aplicații şi site-uri Web necunoscute, despre aplicații rău intenționate şi despre exploatări pe site-uri Web. Rețeaua de protecție în timp real nu urmăreşte activitatea dvs. Web, nu colectează informații despre site-urile Web care au fost deja analizate şi nu colectează informații despre aplicațiile curate care sunt instalate pe computerul dvs.

Dacă nu doriți să contribuiți cu aceste date, Rețeaua de protecție în timp real nu colectează informații despre aplicațiile instalate sau despre site-urile Web vizitate. Cu toate acestea, produsul trebuie să interogheze serverele F-Secure cu privire la reputația aplicațiilor, a site-urilor Web, a mesajelor şi a altor obiecte. Interogarea se efectuează utilizând o sumă de verificare criptografică, în care obiectul interogat nu este trimis la F-Secure. Nu înregistrăm date pentru fiecare utilizator, numai contorul de accesări creşte pentru acel fişier sau site Web.

Nu este posibil să oprim complet tot traficul de rețea către Rețeaua de protecție în timp real, deoarece reprezintă o parte integrantă a protecției oferite de produs.

Avantajele oferite de Rețeaua de protecție în timp real

Cu Rețeaua de protecție în timp real, veți beneficia de o protecție mai rapidă şi mai precisă împotriva celor mai recente amenințări şi nu veți primi alerte inutile pentru aplicații suspecte care nu sunt rău intenționate.

În calitate de colaborator la Rețeaua de protecție în timp real, ne puteți ajuta să găsim malware nou şi nedetectat şi să eliminăm posibilele amenințări false din baza noastră de date cu definiții de viruşi.

Toți participanții la Rețeaua de protecție în timp real se ajută reciproc. Când Rețeaua de protecție în timp real identifică o aplicație suspectă pe dispozitivul dvs., beneficiați de rezultatele analizei efectuate când aceeaşi aplicație a fost identificată deja pe alte dispozitive. Rețeaua de protecție în timp real îmbunătățeşte performanța

generală a dispozitivului dvs., deoarece produsul de securitate instalat nu mai trebuie să scaneze din nou aplicațiile pe care Rețeaua de protecție în timp real le-a analizat şi le-a evaluat ca fiind curate. În mod similar, informațiile despre site-urile Web rău intenționate şi mesajele în bloc nedorite sunt partajate prin Rețeaua de protecție în timp real şi vă putem oferi o protecție mult mai precisă împotriva programelor exploit de pe site-urile Web şi a mesajelor spam.

Cu cât contribuie mai multe persoane la Rețeaua de protecție în timp real, cu atât mai bine sunt protejați participanții individuali.

Cu ce date contribuiți

Ca un colaborator la Rețeaua de protecție în timp real, contribuiți cu informații despre aplicațiile stocate pe dispozitivul dvs. şi despre site-urile Web accesate pentru ca Rețeaua de protecție în timp real să poată furniza protecție împotriva celor mai recente aplicații rău intenționate şi a site-urilor Web suspecte.

Analizarea reputației unui fişier

Rețeaua de protecție în timp real colectează informații numai despre aplicațiile care nu au o reputație cunoscută şi despre fişierele care sunt suspecte sau cunoscute ca fiind programe malware.

Rețeaua de protecție în timp real colectează informații anonime despre aplicațiile curate şi suspecte de pe dispozitivul dvs. Rețeaua de protecție în timp real colectează informații numai despre fişierele executabile (cum ar fi fişierele cu formatul Portable Executable pe platforma Windows, care au extensiile .cpl, .exe, .dll, .ocx, .sys, .scr şi .drv).

Informațiile colectate includ:

- calea fişierului unde se află aplicația pe dispozitivul dvs.;
- dimensiunea fişierului şi data creării sau a modificării;
- atribute şi privilegii fişier;
- informații privind semnătura fişierului;
- versiunea curentă a fişierului şi compania care l-a creat;
- originea fişierului sau URL-ul de descărcare;
- rezultatele analizelor efectuate de F-Secure DeepGuard şi F-Secure Anti-Virus asupra fişierelor scanate;
- alte informații similare.

Rețeaua de protecție în timp real nu colectează niciodată informații privind documentele dvs. personale, decât dacă s-a constatat că sunt infectate. Pentru orice tip de fişier rău intenționat, colectează numele infecției şi starea dezinfecției pentru acel fişier.

Cu Rețeaua de protecție în timp real puteți, de asemenea, trimite aplicațiile suspecte pentru a fi analizate. Aplicațiile trimise includ numai fişiere cu formatul Portable Executable. Rețeaua de protecție în timp real nu colectează niciodată informații privind documentele dvs. personale şi acestea nu sunt niciodată încărcate automat pentru a fi analizate.

Trimiterea fişierelor pentru a fi analizate

Cu Rețeaua de protecție în timp real, puteți trimite, de asemenea, aplicații suspecte pentru analiză.

Puteți trimite manual anumite aplicații suspecte când produsul vă solicită acest lucru. Puteți trimite numai fişiere executabile portabile. Rețeaua de protecție în timp real nu încarcă niciodată documentele dvs. personale.

Analizarea reputației site-urilor Web

Rețeaua de protecție în timp real nu înregistrează activitatea dvs. pe Web şi nu colectează informații despre site-urile Web care au fost deja analizate. Se asigură că site-urile Web accesate sunt sigure în timp ce navigați pe Web. Când accesați un site Web, Rețeaua de protecție în timp real verifică siguranța acestuia şi vă notifică dacă site-ul este evaluat ca suspect sau dăunător.

Dacă site-ul Web accesat include conținut rău intenționat sau suspect ori un program exploit cunoscut, Rețeaua de protecție în timp real colectează URL-ul complet al site-ului pentru a se putea analiza conținutul paginii Web.

Dacă accesați un site care nu a fost încă evaluat, Rețeaua de protecție în timp real colectează numele domeniului şi al subdomeniului şi, în anumite cazuri, calea spre pagina accesată, pentru ca site-ul să poată fi analizat şi evaluat. Toți parametrii adresei URL care ar putea conține informații ce pot face trimitere la dvs. într-un mod identificabil personal sunt eliminați pentru a vă proteja confidențialitatea.

Notă: Rețeaua de protecție în timp real nu evaluează şi nu analizează paginile Web din rețelele private, deci nu va colecta niciodată informații despre adresele IP din rețelele private (de exemplu, rețele de intranet corporatiste).

Analizarea informațiilor de sistem

Rețeaua de protecție în timp real colectează numele şi versiunea sistemului dvs. de operare, informații legate de conexiunea la Internet şi statistici privind utilizarea Rețelei de protecție în timp real (de exemplu, de câte ori s-a interogat reputația unui site Web şi timpul mediu de trimitere a unui rezultat pentru interogare) pentru a putea monitoriza şi îmbunătăți serviciul.

Cum vă protejăm confidențialitatea

Transferăm informațiile într-un mod securizat şi eliminăm automat toate informațiile personale care ar putea fi conținute de date.

Rețeaua de protecție în timp real elimină datele de identificare înainte de a le trimite la F-Secure şi criptează toate informațiile adunate în timpul transferului pentru a le proteja împotriva accesului neautorizat. Informațiile adunate nu sunt procesate individual; sunt grupate cu informațiile de la alți colaboratori la Rețeaua de protecție în timp real. Toate datele sunt analizate statistic şi în mod anonim, ceea ce înseamnă că acestea nu vor fi corelate cu dvs. în niciun fel.

Informațiile care v-ar putea identifica personal nu sunt incluse în datele colectate. Rețeaua de protecție în timp real nu colectează adrese IP private sau informațiile dvs. private, cum ar fi adrese de e-mail, nume de utilizator sau parole. Cu toate că depunem eforturi pentru a elimina toate datele de identificare personală, este posibil ca unele date de identificare să rămână în informațiile colectate. În aceste cazuri, nu vom utiliza datele colectate neintenționat pentru a vă identifica.

Aplicăm măsuri de securitate stricte şi metode de protecție fizice, administrative şi tehnice pentru a proteja informațiile colectate când sunt transferate, stocate şi procesate. Informațiile sunt stocate în locații securizate şi pe servere care sunt controlate de compania noastră, localizate la sediile noastre sau la sediile subcontractanților noştri. Numai personalul autorizat poate accesa informațiile colectate.

F-Secure poate partaja datele colectate cu afiliații, subcontractanții, distribuitorii şi partenerii săi, dar întotdeauna într-un format neidentificabil şi anonim.

Cum deveniți colaborator la Rețeaua de protecție în timp real

Dacă veți contribui cu informații privind programele şi site-urile Web rău intenționate, ne ajutați să îmbunătățim protecția oferită de Rețeaua de protecție în timp real.

Puteți alege să participați la Rețeaua de protecție în timp real în timpul instalării. Cu setările implicite de instalare, contribuiți cu date la Rețeaua de protecție în timp real. Puteți schimba ulterior această setare în produs.

Urmați aceste instrucțiuni pentru a modifica setările Rețelei de protecție în timp real:

1. Pe panoul de lansare, faceți clic dreapta pe pictograma din extrema dreaptă.
   Va apărea un meniu de tip pop-up.
2. Selectați **Deschidere setări comune**.
3. Selectați **Altele** > **Confidențialitate**.

4. Bifați caseta de selectare Participare pentru a deveni colaborator la Rețeaua de protecție în timp real.

Întrebări despre rețeaua de protecție în timp real

Informații de contact pentru întrebările legate de rețeaua de protecție în timp real.

Dacă aveți întrebări suplimentare legate de rețeaua de protecție în timp real, contactați:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finlanda

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

Cea mai recentă versiune a acestei politici este mereu disponibilă pe site-ul nostru Web.

Cum ştiu dacă abonamentul meu este valid

Tipul şi starea abonamentului dvs. sunt afişate pe pagina **Stare abonament**.

Când abonamentul este pe punctul de a expira sau dacă abonamentul a expirat, starea de protecție generală a programului din pictograma corespunzătoare din panoul de lansare se modifică.

Pentru a verifica valabilitatea abonamentului:

1. Pe panoul de lansare, faceți clic dreapta pe pictograma din extrema dreaptă.
   Va apărea un meniu de tip pop-up.
2. Selectați **Vizualizare abonamentele mele**.
3. Selectați **Stare abonament** pentru a vizualiza informații despre abonamentele dvs. pentru programele instalate.
4. Selectați **Stare instalare** pentru a vedea programele disponibile pentru a fi instalate.

Starea abonamentului şi data de expirare a acestuia sunt, de asemenea, afişate pe pagina de **Statistici** a programului. Dacă abonamentul a expirat, trebuie să-l reînnoiți pentru a continua să primiți actualizări şi pentru a utiliza produsul.

Notă: Când abonamentul dvs. a expirat, pictograma de stare a produsului clipeşte în bara de sistem.

Centrul de acțiuni

Centrul de acțiuni vă afişează toate notificările importante care necesită atenția dvs.

Dacă abonamentul a expirat sau este pe cale să expire, centrul de acțiuni vă înştiințează de acest lucru. Culoarea fundalului şi conținutul mesajului centrului de acțiuni depinde de tipul şi de starea abonamentului:

- Dacă abonamentul este pe cale să expire şi există abonamente gratuite disponibile, mesajul conține un fundal alb şi un buton **Activare**.
- Dacă abonamentul este pe cale să expire şi nu există abonamente gratuite disponibile, mesajul conține un fundal galben şi butoanele **Cumpărare** şi **Introducere cheie**. Dacă ați cumpărat deja un nou abonament, puteți face clic pe **Introducere cheie** pentru a furniza cheia de abonament şi pentru a activa noul abonament.

- Dacă abonamentul a expirat şi există abonamente gratuite disponibile, mesajul conține un fundal roşu şi un buton **Activare**.
- Dacă abonamentul a expirat şi nu există abonamente gratuite disponibile, mesajul conține un fundal roşu şi butoanele **Cumpărare** şi **Introducere cheie**. Dacă ați cumpărat deja un nou abonament, puteți face clic pe **Introducere cheie** pentru a furniza cheia de abonament şi pentru a activa noul abonament.

Notă: Linkul **Afişare istoric de notificări** din centrul de acțiuni prezintă o listă cu mesaje de notificare privind produsul, nu mesaje anterioare din centrul de acțiuni.

Activarea abonamentului

Când aveți o cheie nouă de abonament sau un cod nou de campanie pentru un produs, trebuie să le activați.

Pentru a activa un abonament:

1. Pe panoul de lansare, faceți clic dreapta pe pictograma din extrema dreaptă.
   Va apărea un meniu de tip pop-up.
2. Selectați **Vizualizare abonamentele mele**.
3. Alegeți una dintre următoarele:
   - Faceți clic pe **Activare abonament**.
   - Faceți clic pe **Activare cod de campanie**.
4. În caseta de dialog care se deschide, introduceți noua cheie de abonament sau codul de campanie şi faceți clic pe**OK**.

   Sfat: Dacă ați primit cheia de abonament prin e-mail, o puteți copia din mesajul de e-mail şi o puteți lipi în câmp.

După ce ați introdus noua cheie de abonament, data de valabilitate a noului abonament este afişată în pagina **Stare abonament**.

Capitolul

3

Introducere

Subiecte:

- *Vizualizarea stării generale a protecției mele*
- *Vizualizați statisticile produsului*
- *Gestionarea actualizărilor produsului*
- *Ce reprezintă viruşii şi alte programe malware*

Acest produs vă protejează computerul împotriva viruşilor şi a altor aplicații dăunătoare.

Produsul scanează fişiere, analizează aplicații şi realizează actualizări în mod automat. Nu necesită nicio acțiune din partea dvs.

Vizualizarea stării generale a protecției mele

Pagina **Stare** vă afişează o prezentare generală rapidă a caracteristicilor produsului instalat şi starea lor curentă.

Pentru a deschide pagina **Stare**:

În pagina principală, faceți clic pe **Stare**.

Se deschide pagina **Stare**.

Pictogramele vă afişează starea programului şi caracteristicile sale de securitate.

Pictogramă stare	Nume stare	Descriere
	OK	Computerul dvs. este protejat. Caracteristica este activată şi funcționează corespunzător.
	Informații	Produsul vă informează despre starea specială a unei caracteristici. De exemplu, caracteristica este în curs de actualizare.
	Avertisment	Computerul dvs. nu este protejat în totalitate. De exemplu, produsul nu a mai fost actualizat de multă vreme sau starea unei caracteristici necesită atenție.
	Eroare	Computerul dvs. nu este protejat De exemplu, abonamentul dvs. a expirat sau o caracteristică critică este dezactivată.
	Oprit	O caracteristică neimportantă este dezactivată.

Vizualizați statisticile produsului

Puteți vedea ce a făcut produsul de la instalarea sa în pagina **Statistici**.

Pentru a deschide pagina **Statistici**:

În pagina principală, faceți clic pe **Statistici**.

Se deschide pagina **Statistici**.

- **Verificare cea mai recentă actualizare reuşită** afişează ora celei mai recente actualizări.

- **Scanare pentru viruşi şi spyware** afişează numărul de fişiere pe care produsul le-a scanat şi curăţat de la instalare.
- **Aplicaţii** afişează numărul de programe pe care DeepGuard le-a permis sau le-a blocat de la instalare.
- **Conexiuni firewall** afişează numărul de conexiuni permise sau blocate în perioada scursă de la instalare.
- **Filtrarea pentru spam şi înşelăciune** vă arată câte mesaje de e-mail a detectat produsul ca mesaje valide, respectiv ca mesaje spam.

Gestionarea actualizărilor produsului

Produsul asigură actualizarea funcţiei de protecţie în mod automat.

Vizualizarea versiunii bazei de date

Puteţi vedea informaţii despre momentele în care au avut loc actualizări şi despre numerele de versiuni în pagina **Actualizări ale bazei de date**.

Pentru a deschide pagina **Actualizări ale bazei de date**:

1. În pagina principală, faceţi clic pe **Setări**.

   Notă: Pentru a modifica setările, aveţi nevoie de drepturi administrative.

2. Selectaţi **Alte setări** > **Versiuni bază de date**.

Pagina **Versiuni ale bazei de date** afişează cea mai recentă dată la care au fost actualizate definiţiile de viruşi şi spyware, DeepGuard şi filtrarea pentru spam şi înşelăciune, precum şi numerele de versiuni ale acestora.

Modificarea setărilor pentru reţeaua de bandă largă mobilă

Selectaţi dacă doriţi să descărcaţi actualizări de securitate atunci când utilizaţi reţeaua de bandă largă mobilă.

Notă: Această caracteristică este disponibilă doar în Microsoft Windows 7.

Implicit, actualizările de securitate sunt întotdeauna descărcate atunci când sunteţi în reţeaua operatorului de domiciliu. Oricum, actualizările sunt suspendate atunci când vizitaţi reţeaua altui operator. Cauza o reprezintă faptul că preţurile pot varia între operatori, de exemplu, în ţări diferite. Păstraţi această setare neschimbată, dacă vreţi să salvaţi bandă şi posibil bani, în timpul vizitelor dvs.

Notă: Setarea se aplică doar conexiunilor de bandă largă mobilă. Atunci când computerul este conectat la o reţea fixă sau fără fir, produsul este actualizat în mod automat.

Pentru a modifica setarea:

1. În pagina principală, faceţi clic pe **Setări**.

   Notă: Pentru a modifica setările, aveţi nevoie de drepturi administrative.

2. Selectaţi **Alte setări** > **Bandă largă mobilă** > **Descărcare actualizări de securitate**.
3. Selectaţi opţiunea de actualizare preferată pentru conexiunile mobile:
   - **Numai în reţeaua operatorului de domiciliu**

     Actualizările sunt întotdeauna descărcate în reţeaua operatorului de domiciliu. Când vizitaţi reţeaua altui operator, actualizările sunt suspendate. Vă recomandăm să selectaţi această opţiune pentru a menţine securitatea produsului la zi, la costuri previzibile.
   - **Niciodată**

Nu se descarcă actualizări atunci când utilizați banda largă mobilă.

- **Întotdeauna**

  Actualizările sunt descărcate întotdeauna, indiferent de rețeaua pe care o utilizați. Selectați această opțiune dacă doriți să vă asigurați că securitatea computerului este întotdeauna actualizată, indiferent de costuri.

4. Dacă doriți să decideți separat, de fiecare dată când ieşiți din zona operatorului de domiciliu, selectați **Se confirmă de fiecare dată când ieşiți din rețeaua de domiciliu**.

Actualizări de securitate suspendate

Actualizările de securitate pot fi suspendate atunci când utilizați rețeaua de bandă largă mobilă în afara rețelei operatorului de domiciliu.

În acest caz, puteți vedea fluturaşul de notificare **Suspendat** în colțul din dreapta jos al ecranului. Actualizările sunt suspendate, deoarece prețurile conexiunilor pot varia, de exemplu, între operatorii din diferite țări. Vă recomandăm să lăsați această setare nemodificată dacă doriți să economisiți lățimea de bandă şi posibil şi costurile în timpul vizitei. Totuşi, dacă încă doriți să modificați setările, faceți clic pe linkul **Modificare**.

Notă:

Această caracteristică este disponibilă doar în Microsoft Windows 7.

Ce reprezintă viruşii şi alte programe malware

Malware reprezintă programe proiectate specific pentru a vă deteriora computerul, pentru a vă utiliza computerul în scopuri ilegale fără să ştiți acest lucru sau pentru a fura informații din computer.

Malware-ul poate:

- să preia controlul asupra browser-ului Web,
- să vă redirecționeze încercările de căutare,
- să afişeze publicitate nedorită,
- să urmărească ce site-uri Web ați vizitat,
- să vă fure informații personale cum ar fi cele despre conturi bancare,
- să vă utilizeze computerul pentru a trimite spam şi
- să vă utilizeze computerul pentru a ataca alte computere.

Malware-ul poate, de asemenea, să încetinească şi să destabilizeze computerul. Este posibil să bănuiți că aveți *malware* pe computer, dacă acesta merge încet dintr-o dată şi se strică adesea.

Viruşi

Viruşii sunt, de regulă, programe care se pot ataşa singure la fişiere şi se pot clona în mod repetat; viruşii pot altera şi pot înlocui conținutul altor fişiere într-un mod în care computerul poate fi afectat negativ.

Un *virus* este un program care, în mod normal, s-a instalat în computer fără să ştiți. Odată ajuns în computer, virusul va încerca să se auto-cloneze. Virusul:

- utilizează anumite resurse de sistem ale computerului,
- poate altera sau poate deteriora fişiere din computer,
- încearcă probabil să vă utilizeze computerul pentru a infecta alte computere,
- îi poate permite computerului să fie utilizat în scopuri ilegale.

Spyware

Spyware-ul este un program care colectează informații personale.

Programele spyware pot colecta informații personale care includ:

- Site-urile de Internet pe care ați navigat,
- adresele de e-mail din computer,
- parole sau
- numere de cărți de credit.

Programele spyware se instalează aproape întotdeauna singure, fără permisiunea dvs. explicită. Spyware-ul se poate instala împreună cu un alt program folositor sau înşelându-vă să faceți clic pe o opțiune dintr-o fereastră pop-up.

Programe rootkit

Programele rootkit sunt acelea care fac ca alte programe *malware* să fie greu de depistat.

Programele rootkit ascund fişiere şi procese. În general, acestea procedează astfel pentru a ascunde o activitate rău intenționată de pe computer. Atunci când un program rootkit ascunde un element *malware*, va fi mai greu să descoperiți că în computer există malware.

Acest produs are un scaner de programe rootkit care scanează în mod special după programe rootkit, astfel încât ascunderea elementelor *malware* să fie mai dificilă.

Riskware

Riskware-ul nu este proiectat special pentru a afecta negativ computerul, dar poate dăuna dacă este incorect utilizat.

Programul riskware nu este un malware în sensul strict al cuvântului. Programele riskware efectuează anumite funcții utile, dar potențial periculoase.

Exemple de programe riskware:

- programe de mesagerie instantanee, cum ar fi IRC (Internet relay chat),
- programe pentru transferul fişierelor prin Internet de la un computer la altul,
- sau programe de telefonie prin Internet, cum ar fi VoIP (*Voce prin protocol Internet*).
- software de acces la distanță, cum ar fi VNC,
- scareware, care poate încerca să sperie sau să păcălească persoane pentru a cumpăra software de securitate fals sau
- software destinat să ocolească verificările de pe CD sau să copieze protecțiile.

Dacă ați instalat explicit programul şi l-ați configurat corect, este puțin probabil ca acesta să fie dăunător.

Dacă elementul riskware a fost instalat fără să ştiți, a fost instalat cel mai probabil cu rea intenție, deci ar trebui eliminat.

Capitolul

4

Protejarea computerului împotriva programelor malware

Subiecte:

- *Cum pot scana computerul meu*
- *Cum excludeți fişiere din scanare*
- *Cum puteți utiliza carantina*
- *Ce reprezintă DeepGuard*

Caracteristica Scanare pentru viruşi şi spyware protejează computerul împotriva programelor care pot fura informații personale, pot deteriora computerul sau îl pot utiliza în scopuri ilegale.

În mod implicit, toate tipurile de malware sunt manevrate imediat când sunt găsite, astfel încât acestea să nu afecteze în mod negativ computerul.

În mod implicit, caracteristica Scanare viruşi şi spyware scanează unitățile de disc locale, suporturile media amovibile (de ex., discurile portabile sau cd-urile) şi conținutul descărcat în mod automat. De asemenea, puteți să configurați funcția pentru a scana în mod automat şi mesajele de poştă electronică.

Caracteristica Scanare pentru viruşi şi spyware monitorizează, de asemenea, orice schimbări din computerul dvs. care pot indica *malware*. Dacă sunt găsite modificări periculoase de sistem, de exemplu, ale configurărilor de sistem sau încercări de modificare a proceselor importante de sistem, DeepGuard opreşte programul să fie executat, deoarece este posibil să fie *malware*.

Cum pot scana computerul meu

Când caracteristica Scanare pentru viruşi şi spyware este activată, ea caută în mod automat fişierele dăunătoare de pe computerul dvs. Puteți, de asemenea, să realizați o scanare manuală sau să configurați scanări programate.

Vă recomandăm să țineți caracteristica Scanare pentru viruşi şi spyware activată tot timpul. Scanați fişierele manual atunci când doriți să vă asigurați că nu există fişiere dăunătoare pe computer sau dacă doriți să scanați fişiere pe care le-ați exclus din scanarea în timp real.

Prin configurarea unei scanări programate, Caracteristica Scanare pentru viruşi şi spyware elimină fişierele dăunătoare de pe computer în anumite momente specificate.

Scanați fişierele în mod automat

Scanarea în timp real vă protejează computerul scanând toate fişierele atunci când sunt accesate şi blocând accesul la acele fişiere care conțin *malware*.

Când computerul dvs. încearcă să acceseze un fişier, scanarea în timp real scanează fişierul împotriva malware-ului înainte de a permite computerului să acceseze fişierul. Dacă scanarea în timp real găseşte conținut dăunător, pune fişierul în carantină, înainte ca acesta să poată strica ceva.

Scanarea în timp real afectează performanța computerului?

În mod normal, nu veți observa procesul de scanare, deoarece acesta durează puțin timp şi consumă puține resurse de sistem. Perioada de timp şi resursele de sistem consumate de Scanarea în timp real depind, de exemplu, de conținutul, de locația şi de tipul fişierului.

Fişiere a căror scanare durează mai mult:

- Fişierele de pe unitățile amovibile, de exemplu, CD-uri, DVD-uri şi de pe unitățile USB portabile.
- Fişierele comprimate, precum fişierele *.zip* fişiere.

  Notă: Fişierele comprimate nu sunt scanate în mod implicit.

Este posibil ca Scanarea în timp real să vă încetinească computerul dacă:

- aveți un computer care nu îndeplineşte cerințele de sistem sau
- accesați o mulțime de fişiere în acelaşi timp. De exemplu, când deschideți un director care conține multe fişiere care trebuie scanate.

Activarea sau dezactivarea scanării în timp real

Țineți scanarea în timp real activată pentru a opri programele *malware* înainte de a dăuna computerului.

Pentru a activa şi dezactiva scanarea în timp real:

1. În pagina principală, faceți clic pe **Stare**.
2. Faceți clic pe **Modificare setări în această pagină**.

   Notă: Aveți nevoie de drepturi administrative pentru a dezactiva caracteristicile de securitate.

3. Activați şi dezactivați caracteristica **Scanare pentru viruşi şi spyware**.
4. Faceți clic pe **Închidere**.

Manevrarea automată a fişierelor dăunătoare

Scanarea în timp real poate să manevreze fişierele dăunătoare în mod automat, fără să vă pună nicio întrebare.

Pentru a seta scanarea în timp real să manevreze fişierele dăunătoare în mod automat:

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Selectați **Securitate computer** > **Scanare pentru viruşi şi spyware**.
3. Selectați **Manevrare automată a fişierelor dăunătoare**.

Dacă alegeți ca fişierele dăunătoare să nu fie manevrate în mod automat, scanarea în timp real vă întreabă ce să facă de fiecare dată când găseşte un fişier dăunător.

Gestionați spyware-ul

Caracteristica Scanare pentru viruşi şi spyware blochează spyware-ul imediat ce încearcă să se execute.

Înainte ca o aplicație spyware să poată fi executată, produsul o blochează şi vă permite să decideți ce faceți cu ea.

Alegeți una dintre următoarele acțiuni pentru a se realiza la găsirea unei aplicații spyware:

Acțiune de efectuat	Ce se întâmplă cu programul spyware
Manevrare automată	Lăsați produsul să decidă cea mai bună acțiune de efectuat, în funcție de ce spyware a găsit.
Mutați spyware-ul în carantină	Mutați spyware-ul în carantină, de unde nu va putea dăuna computerului.
Ştergeți spyware-ul	Eliminați toate fişierele de tip spyware de pe computer.
Doar blocați spyware-ul	Blocați accesul la spyware dar îl lăsați pe computer.
Excludeți spyware-ul din scanare	Permiteți spyware-ului să se execute şi îl excludeți din scanările viitoare.

Gestionați riskware-ul

Caracteristica Scanare pentru viruşi şi spyware blochează programele clasificate ca riskware imediat ce se încearcă executarea acestora.

Înainte ca o aplicație riskware să poată fi executată, produsul o blochează şi vă permite să decideți ce faceți cu ea.

Alegeți una dintre următoarele acțiuni pentru a se realiza la găsirea unei aplicații riskware:

Acțiune de efectuat	Ce se întâmplă cu programele riskware
Doar blocați riskware-ul	Blocați accesul la riskware dar îl lăsați pe computer.
Mutați riskware-ul în carantină	MovMutați riskware-ul în carantină, de unde nu va putea dăuna computerului.
Ştergeți riskware-ul	Eliminați toate fişierele de tip riskware de pe computer.
Excludeți riskware-ul din scanare	Permiteți riskware-ului să se execute şi îl excludeți din scanările viitoare.

Eliminați în mod automat modulele cookie de urmărire

Eliminând modulele cookie de urmărire, opriți posibilitatea site-urilor Web de a urmări parcursul dvs. pe Internet.

Modulele cookie de urmărire sunt mici fişiere care permit site-urilor Web să înregistreze parcursul vizitelor dvs. Urmați aceste instrucțiuni pentru a ține modulele cookie departe de computerul dvs.

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Selectați **Securitate computer** > **Scanare pentru viruşi şi spyware**.
3. Selectați **Eliminare module cookie de urmărire**.
4. Faceți clic pe **OK**.

Scanați manual fişierele

Puteți să scanați manual fişierele, de exemplu atunci când conectați un dispozitiv extern la computer, pentru a vă asigura că acesta nu conține malware.

pornirea scanării manuale

Puteți scana întregul computer sau pentru un anumit tip de *malware* sau o anumită locație.

Dacă suspectați existența unui anumit tip de *malware*, puteți scana numai pentru acest tip. Dacă suspectați o anumită locație din computer, puteți scana numai secțiunea respectivă. Aceste scanări se vor termina mult mai repede decât o scanare a întregului computer.

Pentru a porni scanarea manuală a computerului:

1. În pagina principală, faceți clic pe săgeata de sub **Scanare**.

   Se afişează opțiunile de scanare.

2. Selectați tipul de scanare.

   Selectați **Modificare setări scanare** pentru a optimiza modul în care scanarea manuală caută viruşi şi alte aplicații dăunătoare pe computerul dvs.

3. Dacă ați selectat **Alegere pentru scanare**, se deschide o fereastră în care puteți selecta ce locație să scanați.
   Se deschide **Expert scanare**.

Tipuri de scanare

Puteți scana întregul computer sau pentru un anumit tip de malware sau o anumită locație.

Se prezintă diferitele tipuri de scanare:

Tip de scanare	Ce este scanat	Când se utilizează acest tip
Scanare pentru viruşi şi spyware	Părți ale computerului dvs. pentru detectarea de viruşi, spyware şi riskware	Acest tip de scanare este mult mai rapid decât scanarea completă. Verifică doar părțile din sistem care conțin fişiere program instalate. Acest tip de scanare este recomandat dacă doriți o verificare rapidă a computerului, deoarece poate identifica cu eficiență şi elimina orice program malware de pe computer.
Scanare completă computer	Întregul computer (unități de hard disk interne şi externe) pentru detectarea de viruşi, spyware şi riskware	Când doriți să fiți complet sigur că nu există deloc malware sau riskware în computer. Acest tip de scanare durează cel mai mult pentru a se finaliza. Combină scanarea rapidă pentru detectarea de malware şi scanarea unității de hard disc. Verifică, de asemenea, existența elementelor posibil ascunse de programele rootkit.
Alegere pentru scanare	Un anumit fişier, folder sau unitate pentru detectare de viruşi, spyware şi riskware	Când bănuiți că o anumită locație din computer poate conține malware, de exemplu, locația conține descărcări de la surse potențial periculoase, cum ar fi rețele de

Tip de scanare	Ce este scanat	Când se utilizează acest tip
		partajare a fişierelor peer-to-peer. Durata scanării este în funcție de dimensiunea destinației de scanat. Scanarea se termină rapid dacă, de exemplu, scanați un folder ce conține numai câteva fişiere mici.
Scanare programe rootkit	Locațiile importante din sistem, în care un element suspect poate să însemne o problemă de securitate. Scanează fişiere, foldere, unități sau procese ascunse	Dacă suspectați că un program rootkit poate fi instalat pe computer. De exemplu, dacă un malware a fost detectat de curând pe computerul dvs. şi doriți să vă asigurați că nu a instalat un rootkit.

Scanarea în Windows Explorer

Puteți să scanați discuri, foldere şi fişiere pentru detectare de *viruşi*, *spyware* şi *riskware*, din Windows Explorer.

Pentru a scana un disc, un folder sau un fişier:

1. Plasați indicatorul mouse-ului pe discul, folderul sau fişierul pe care doriți să îl scanați şi faceți clic dreapta.
2. Din meniul apărut prin clic dreapta, selectați **Scanare foldere pentru detectare de viruşi**. (Numele opțiunii depinde de ceea ce scanați: un disc, un folder sau un fişier.)
   Se deschide fereastra **Expert scanare** şi începe procesul de scanare.

Dacă se găseşte un *virus* sau un *spyware*, **Expert scanare** vă ghidează prin etapele de curățare.

Selectarea fişierelor de scanat

Puteți selecta tipurile de fişiere care doriți să fie scanate pentru detectare de *viruşi* şi *spyware* în scanările manuale sau programate.

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Selectați **Alte setări** > **Scanare manuală**.
3. În **Opțiuni scanare**, selectați dintre următoarele setări:

Scanare numai tipuri cunoscute de fişiere	Pentru a scana numai acele tipuri de fişiere care conțin cel mai probabil infecții, de exemplu, fişierele executabile. Selectarea acestei opțiuni face şi scanarea mai rapidă. Sunt scanate fişierele cu următoarele extensii: `.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`, and `.hqx`.
Scanare în interiorul fişierelor comprimate	Pentru a scana fişiere sau foldere din arhivă.

Utilizare euristică avansată	Pentru a utiliza toți algoritmii euristici disponibili în timpul scanării pentru a găsi mai bine malware-ul nou sau necunoscut. **Notă:** Dacă selectați această opțiune, scanarea durează mai mult şi poate duce la mai multe valori pozitive false (fişiere nedăunătoare raportate ca suspecte).

4. Faceți clic pe **OK**.

Notă: Fişierele excluse, care se află pe lista de elemente excluse, nu se vor scana, chiar dacă le selectați aici pentru scanare.

Ce să se întreprindă la găsirea unor fişiere dăunătoare

Selectați cum doriți să se manevreze fişierele dăunătoare atunci când sunt descoperite.

Pentru a selecta ce acțiune să aibă loc atunci când se descoperă conținut dăunător în timpul scanării manuale:

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Selectați **Alte setări** > **Scanare manuală**.
3. În **Când se detectează viruşi sau spyware**, alegeți dintre următoarele opțiuni:

Opțiune	Descriere
Să fiu întrebat (implicit)	Puteți să selectați acțiunea care se realizează, pentru fiecare element găsit în timpul scanării manuale.
Curățare fişiere	Produsul încearcă în mod automat să dezinfecteze fişierele infectate pe care le găseşte în timpul scanării manuale. **Notă:** Dacă produsul nu poate curăța un fişier infectat, îl plasează în carantină (cu excepția cazurilor în care acesta este găsit în rețea sau pe un disc amovibil), astfel încât să nu poată să mai dăuneze computerului.
Plasare fişiere în carantină	Produsul mută în carantină toate fişierele dăunătoare pe care le găseşte în timpul scanării manuale, astfel încât să nu poată să mai dăuneze computerului.
Ştergere fişiere	Produsul şterge toate fişierele dăunătoare pe care le găseşte în timpul scanării manuale.
Numai raportare	Produsul lasă fişierele dăunătoare pe care le găseşte în timpul scanării manuale aşa cum sunt şi înregistrează detectarea în raportul de scanare. **Notă:** Dacă scanarea în timp real este dezactivată, orice malware poate afecta în continuare negativ computerul dacă selectați această opțiune.

Notă: Când se găsesc fişiere dăunătoare în timpul unei scanări programate, acestea sunt curățate în mod automat.

Programarea unei scanări

Setați computerul astfel încât acesta să elimine în mod automat viruşii şi alte aplicații dăunătoare, atunci când nu îl utilizați, sau setați-l să execute periodic scanarea, pentru a vă asigura că aveți un computer curat.

Pentru a programa o scanare:

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Selectați **Alte setări** > **Scanare programată**.
3. Activați caracteristica **Scanare programată**.
4. Selectați momentul în care ați dori să se realizeze scanarea.

Opțiune	Descriere
Zilnic	Scanați computerul zilnic.
Săptămânal	Scanați computerul în anumite zile ale săptămânii. Selectați zilele din listă.
Lunar	Scanați computerul în anumite zile ale lunii. Pentru a selecta zilele: 1. Selectați una dintre opțiunile **Zi**. 2. Selectați ziua din lună din lista de lângă ziua selectată.

5. Selectați când doriți să pornească scanarea în zilele selectate.

Opțiune	Descriere
Oră de început	Porniți scanarea la o anumită oră.
După neutilizarea computerului pentru	Porniți scanarea după ce nu ați utilizat computerul pentru o perioadă specificată de timp.

Scanarea programată utilizează setările de scanare manuală, cu excepția faptului că scanează arhivele de fiecare dată şi şterge fişierele dăunătoare în mod automat.

Scanarea e-mailurilor

Scanarea e-mailurilor vă protejează împotriva fişierelor dăunătoare trimise prin e-mail.

Pentru căutarea viruşilor în mesajele de e-mail, Scanarea pentru viruşi şi spyware trebuie să fie activată.

Pentru a activa scanarea e-mailurilor:

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Selectați **Securitate computer** > **Scanare pentru viruşi şi spyware**.
3. Selectați **Eliminare ataşări dăunătoare din e-mailuri**.
4. Faceți clic pe **OK**.

Când sunt scanate mesajele şi ataşările mesajelor de e-mail

Scanarea pentru viruşi şi spyware poate să elimine conținutul dăunător din mesajele de e-mail pe care le primiți.

Scanarea pentru viruşi şi spyware elimină mesajele de e-mail dăunătoare primite prin programe de e-mail, precum Microsoft Outlook şi Outlook Express, Microsoft Mail sau Mozilla Thunderbird. Sunt scanate mesajele şi ataşările de e-mail necriptate, de fiecare dată când programul de e-mail le primeşte de la un server care utilizează protocolul POP3.

Caracteristica Scanare pentru viruşi şi spyware nu poate scana mesajele de e-mail accesate prin browser cu aplicații precum Hotmail, Yahoo! mail sau Gmail. Sunteți totuşi protejat împotriva *viruşilor* chiar dacă ataşările dăunătoare nu sunt eliminate din mesajele accesate prin browser. Când descărcați ataşările de e-mail, scanarea în timp real le elimină de pe computer înainte să provoace vreo stricăciune.

Notă: Scanarea în timp real vă protejează doar computerul, nu şi prietenii. Aceasta nu scanează fişierele ataşate decât atunci când le descărcați. Aceasta înseamnă că dacă redirectați un mesaj, este posibil să trimiteți un e-mail infectat către prietenii dvs.

Vizualizarea rezultatelor scanării

Istoricul privitor la viruşi şi spyware afişează toate fişierele dăunătoare pe care le-a găsit produsul.

Uneori, când găseşte ceva dăunător, produsul nu poate să realizeze acțiunea pe care ați selectat-o. De exemplu, dacă ați selectat să se curețe fişierele iar un fişier nu poate fi curățat, produsul mută fişierul în carantină. Puteți vizualiza această informație în istoricul privitor la viruşi şi spyware.

Pentru a vizualiza istoricul:

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Selectați **Securitate computer** > **Scanare pentru viruşi şi spyware**.
3. Faceți clic pe **Vizualizare istoric eliminări**.

Istoricul privitor la viruşi şi spyware afişează următoarele informații:

- data şi ora la care a fost găsit fişierul dăunător,
- numele programului malware şi locația acestuia de pe computer şi
- acțiunea realizată.

Cum excludeți fişiere din scanare

Uneori puteți dori să excludeți din scanare unele fişiere sau aplicații. Elementele excluse nu vor fi scanate până nu le eliminați din lista de elemente excluse.

Notă: Listele de excludere sunt separate pentru scanarea în timp real, respectiv pentru cea manuală. De exemplu, dacă doriți să excludeți un fişier din scanarea în timp real, acesta va fi scanat în timpul scanării manuale, dacă nu îl excludeți şi din aceasta.

Excluderea tipurilor de fişiere

Când excludeți fişiere în funcție de tip, fişierele cu extensiile specificate nu sunt scanate în căutarea vreunui conținut dăunător.

Pentru a adăuga sau elimina tipuri de fişiere pe care doriți să le excludeți:

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Alegeți dacă doriți să excludeți tipul de fişier din scanarea în timp real, respectiv din cea manuală:
   - Selectați **Securitate computer** > **Scanare pentru viruşi şi spyware**, pentru a exclude tipul respectiv de fişier din scanarea în timp real.
   - Selectați **Alte setări** > **Scanare manuală**, pentru a exclude tipul respectiv de fişier din scanarea manuală.
3. Faceți clic pe **Excludere fişiere din scanare**.
4. Pentru a exclude un tip de fişier:
   a) Selectați fila **Tipuri de fişier**.

b) Selectați **Excludere fişiere cu extensiile**.
c) Tastați o extensie de fişier, care identifică tipul fişierelor pe care doriți să le excludeți, în câmpul de lângă butonul **Adăugare**.

   Pentru a specifica fişiere fără nicio extensie, tastați „.”. Puteți utiliza metacaracterul „?” pentru a reprezenta orice caracter unic sau „*” pentru a reprezenta orice număr de caractere.

   De exemplu, pentru a exclude fişierele executabile, tastați `exe` în câmp.
d) Faceți clic pe **Adăugare**.

5. Repetați pasul anterior pentru orice altă extensie pe care doriți să o excludeți de la scanarea pentru detectare de viruşi.
6. Faceți clic pe **OK** pentru a închide caseta de dialog **Excludere din scanare**.
7. Faceți clic pe **OK** pentru a aplica noile setări.

Tipurile de fişiere selectate vor fi excluse din scanările viitoare.

Excluderea fişierelor după locație

Când excludeți fişiere în funcție de locație, fişierele din unitățile şi folderele specificate nu sunt scanate în căutarea vreunui conținut dăunător.

Pentru a adăuga sau elimina locații de fişiere pe care doriți să le excludeți:

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Alegeți dacă doriți să excludeți locația din scanarea în timp real, respectiv din cea manuală:
   - Selectați **Computer** > **Scanare pentru viruşi şi spyware** pentru a exclude locația din scanarea în timp real.
   - Selectați **Computer** > **Scanare manuală** pentru a exclude locația din scanarea manuală.
3. Faceți clic pe **Excludere fişiere din scanare**.
4. Pentru a exclude un fişier, o unitate sau un folder:
   a) Selectați fila **Obiecte**.
   b) Selectați **Excludere obiecte (fişiere, foldere, ...)**.
   c) Faceți clic pe **Adăugare**.
   d) Selectați fişierul, unitatea sau folderul pe care doriți să le excludeți de la scanarea pentru detectare de viruşi.

      Notă: Anumite unități pot fi unități amovibile, cum ar fi CD, DVD sau unități de rețea. Unitățile de rețea şi unitățile amovibile goale nu pot fi excluse.

   e) Faceți clic pe **OK**.
5. Repetați pasul anterior pentru a exclude alte fişiere, unități sau foldere de la scanarea pentru detectare de viruşi.
6. Faceți clic pe **OK** pentru a închide caseta de dialog **Excludere din scanare**.
7. Faceți clic pe **OK** pentru a aplica noile setări.

Fişierele, unitățile sau folderele selectate vor fi excluse din scanările viitoare.

Vizualizarea aplicațiilor excluse

Puteți să vizualizați aplicațiile pe care le-ați exclus din scanare şi să le eliminați din lista de elemente excluse, dacă doriți să fie scanate în viitor.

Dacă scanarea în timp real sau cea manuală detectează o aplicație care se comportă ca un spyware sau un riskware dar dvs. o cunoaşteți ca fiind sigură, o puteți exclude din scanare, astfel încât produsul să nu vă mai avertizeze despre aplicația respectivă.

Notă: Dacă aplicația se comportă ca un virus sau ca alt tip de software rău intenționat, nu poate fi exclusă.

Nu puteți exclude aplicațiile direct. În lista de excludere apar aplicații noi numai dacă le excludeți în timpul scanării.

Pentru a vizualiza aplicațiile excluse din scanare:

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Alegeți dacă doriți să vizualizați aplicațiile care au fost excluse în timpul unei scanări în timp real sau al unei scanări manuale:
   - Selectați **Computer** > **Scanare pentru viruşi şi spyware** pentru a vedea aplicațiile care au fost excluse din scanarea în timp real.
   - Selectați **Computer** > **Scanare manuală** pentru a vizualiza aplicațiile care au fost excluse din scanarea manuală.
3. Faceți clic pe **Excludere fişiere din scanare**.
4. Selectați fila **Aplicații**.

   Notă: Pot fi excluse doar aplicațiile spyware şi riskware, nu viruşii.

5. Dacă doriți să scanați din nou o aplicație exclusă:
   a) Selectați aplicația pe care doriți să o includeți în scanare.
   b) Faceți clic pe **Eliminare**.
6. Faceți clic pe **OK** pentru a închide caseta de dialog **Excludere din scanare**.
7. Faceți clic pe **OK** pentru a ieşi.

Cum puteți utiliza carantina

Carantina reprezintă un depozit sigur pentru fişierele care pot fi dăunătoare.

Fişierele în carantină nu se pot răspândi şi nu vă pot afecta negativ computerul.

Puteți să introduceți în carantină programele *malware*, *spyware* şi *riskware*, pentru a le face inofensive. Dacă va fi necesar, veți putea restaura ulterior aplicații sau fişiere aflate în carantină.

Dacă un element aflat în carantină nu vă este necesar, îl puteți şterge. Ştergerea unui element din carantină îl va elimina permanent din computer.

- În general, orice *malware* aflat în carantină se poate şterge.
- În majoritatea cazurilor, puteți şterge orice *spyware* aflat în carantină. Este posibil ca elementul *spyware* aflat în carantină să facă parte dintr-un program software valabil, iar eliminarea acestuia să oprească funcționarea corectă a programului respectiv. Dacă doriți să păstrați programul în computer, puteți restaura elementele *spyware* aflate în carantină.
- Elementele *riskware* aflate în carantină pot fi programe software legitime. Dacă programul a fost instalat şi configurat de către dvs., puteți să îl restaurați din carantină. Dacă elementul *riskware* a fost instalat fără cunoştința dvs., este cel mai probabil să fi fost instalat cu rea intenție, deci trebuie şters.

Vizualizare elemente din carantină

Puteți vizualiza mai multe informații despre elementele aflate în carantină.

Pentru a vizualiza informații detaliate despre elementele aflate în carantină:

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Selectați **Securitate computer** > **Scanare pentru viruşi şi spyware**.
3. Faceți clic pe **Vizualizare carantină**.
   Pagina **Carantină** afişează numărul total de elemente stocate în carantină.
4. Pentru a vizualiza informații detaliate despre elementele din carantină, faceți clic pe **Detalii**.

   Puteți sorta conținutul fie după numele programului rău intenționat, fie după calea fişierului.

   Se afişează o listă cu primele 100 de elemente cu tipul de elemente din carantină, numele acestora şi calea unde au fost instalate fişierele.
5. Pentru a vizualiza mai multe informații despre un element din carantină, faceți clic pe pictograma de lângă elementul din coloana **Stare**.

Restabilirea elementelor din carantină

Puteți restabili elementele din carantină de care aveți nevoie.

Puteți restabili aplicații sau fişiere din carantină, dacă vă sunt necesare. Nu restabiliți elemente din carantină, decât dacă sunteți sigur că elementele respective nu reprezintă nicio amenințare. Elementele restabilite se mută înapoi în locația lor originală din computer.

Pentru a restabili elementele din carantină:

1. În pagina principală, faceți clic pe **Setări**.

   Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Selectați **Securitate computer** > **Scanare pentru viruşi şi spyware**.
3. Faceți clic pe **Vizualizare carantină**.
4. Selectați elementele din carantină pe care doriți să le restabiliți.
5. Faceți clic pe **Restabilire**.

Ce reprezintă DeepGuard

DeepGuard analizează conținutul fişierelor şi comportamentul aplicațiilor şi monitorizează aplicațiile care nu sunt de încredere.

DeepGuard blochează *viruşii*, *viermii* şi alte aplicații dăunătoare, noi sau nerecunoscute, care încearcă să facă modificări pe computer şi împiedică aplicațiile suspecte să acceseze Internetul.

Când detectează o nouă aplicație care încearcă să facă modificări potențial dăunătoare sistemului, DeepGuard permite aplicației să se execute într-o zonă sigură. În zona sigură, aplicația nu poate dăuna computerului. DeepGuard analizează ce fel de modificări încearcă aplicația să facă şi, în baza analizei, decide cât este de probabil ca aplicația să fie de tip *malware*. Dacă probabilitatea să fie *malware* este ridicată, DeepGuard blochează aplicația.

Modificările potențial dăunătoare pe care DeepGuard le detectează includ:

- modificări de setare a sistemului (Windows registry),
- încercări de dezactivare a programelor de sistem importante, de exemplu a programelor de securitate cum ar fi acest produs,
- încercări de editare a fişierelor de sistem importante.

Activați şi dezactivați DeepGuard

Țineți caracteristica DeepGuard activată pentru a împiedica aplicațiile suspecte să facă modificări potențial dăunătoare asupra sistemului de operare al computerului dvs.

Dacă aveți Windows XP, asigurați-vă că aveți pachetul Service Pack 2 instalat, înainte de a activa DeepGuard.

Pentru a activa şi dezactiva DeepGuard:

1. În pagina principală, faceți clic pe **Stare**.
2. Faceți clic pe **Modificare setări în această pagină**.

   Notă: Aveți nevoie de drepturi administrative pentru a dezactiva caracteristicile de securitate.

3. Activați şi dezactivați **DeepGuard**.
4. Faceți clic pe **Închidere**.

Permiteți executarea aplicațiilor pe care DeepGuard le-a blocat

Puteți să vă exercitați controlul în privința aplicațiilor pe care DeepGuard le permite sau le blochează.

Uneori DeepGuard poate să blocheze executarea unei aplicații sigure, chiar dacă dvs. doriți să o utilizați şi ştiți că este sigură. Acest lucru se întâmplă când aplicația încearcă să facă modificări ale sistemului, care ar putea fi dăunătoare. Este posibil, de asemenea, ca dvs. să o fi blocat neintenționat, răspunzând greşit la un pop-up pe care DeepGuard l-a afişat la un moment dat.

Pentru a permite executarea unei aplicații pe care DeepGuard a blocat-o:

1. Pe pagina principală, faceți clic pe **Instrumente**.
2. Faceți clic pe **Aplicații**.
   Se afişează lista **Aplicații monitorizate**.
3. Găsiți aplicația a cărei executare doriți să o permiteți.

   Notă: Puteți să faceți clic pe titlurile coloanelor pentru a sorta lista. De exemplu, faceți clic pe coloana **Permisiune** pentru a sorta lista în grupuri de programe permise, respectiv respinse.

4. Selectați **Permitere** în coloana **Permisiune**.
5. Faceți clic pe **Închidere**.

DeepGuard permite iar aplicației să facă modificări ale sistemului.

Utilizarea DeepGuard în modul de compatibilitate

Pentru protecție maximă, DeepGuard modifică temporar programele aflate în execuție. Unele programe se autoverifică pentru a se asigura că nu sunt deteriorate sau modificate şi ar putea să nu fie compatibile cu această caracteristică. De exemplu, jocurile online care au instrumente anti-cheating îşi verifică propriul cod la lansarea în execuție, pentru a se asigura că nu a fost modificat în niciun fel. În astfel de situații, puteți să activați modul de compatibilitate.

Pentru a activa modul de compatibilitate:

1. În pagina principală, faceți clic pe **Setări**.

Notă: Pentru a modifica setările, aveți nevoie de drepturi administrative.

2. Selectați **Securitate computer** > **DeepGuard**.
3. Selectați **Se utilizează modul compatibil**.
4. Faceți clic pe **OK**.

Ce este de făcut în cazul avertismentelor de comportament suspect

DeepGuard monitorizează aplicațiile care nu sunt de încredere. Dacă o aplicație monitorizată încearcă să acceseze Internetul, încearcă să modifice sistemul sau se comportă într-un mod suspect, DeepGuard o blochează.

Dacă ați selectat **Să fiu avertizat despre comportamente suspecte** în setările DeepGuard, DeepGuard vă notifică atunci când detectează o aplicație potențial dăunătoare sau când porniți o aplicație a cărei reputație este necunoscută.

Pentru a decide ce doriți să faceți cu aplicația pe care a blocat-o DeepGuard:

1. Faceți clic pe **Detalii** pentru a vizualiza mai multe informații despre program.
   Secțiunea de detalii vă arată:
   - locația aplicației,
   - reputația aplicației în Rețeaua de protecție în timp real şi
   - cât de comună este aplicația.
2. Decideți dacă acordați încredere aplicației pe care a blocat-o DeepGuard:
   - Alegeți **Am încredere în aplicație. Poate continua.** dacă nu doriți să blocați aplicația.

     Aplicația este probabil sigură dacă:
     - DeepGuard a blocat aplicația în urma unei operațiuni efectuate de dvs,,
     - recunoaşteți aplicația sau
     - ați obținut aplicația dintr-o sursă de încredere.
   - Alegeți **Nu am încredere în aplicație. Se păstrează blocată.** dacă doriți ca aplicația să rămână blocată.

     Aplicația este probabil nesigură dacă:
     - nu este o aplicație comună,
     - aplicația are o reputație necunoscută sau
     - nu cunoaşteți aplicația.
3. Dacă doriți să remiteți o aplicație suspectă spre analiză:
   a) Faceți clic pe **Raportați această aplicație la F-Secure**.
   Produsul afişează condițiile de remitere.
   b) Faceți clic pe **Acceptare** dacă sunteți de acord cu condițiile şi doriți să remiteți eşantionul.

   Vă recomandăm să remiteți un eşantion atunci când:
   - DeepGuard blochează o aplicație despre care ştiți că ar fi sigură sau
   - suspectați că aplicația ar putea fi de tip *malware*.