INTERNET SECURITY 2013

Manual de utilizare

Bitdefender Internet Security 2013
Manual de utilizare

Publicat 16.07.2012

Termeni legali


Bitdefender

Cuprins

Instalare

1. Pregătirea pentru instalare

Pentru a instala Bitdefender Internet Security 2013 fără probleme, parcurgeți acești pași prealabili:

- Asigurați-vă că sistemul pe care doriți să instalați Bitdefender întrunește cerințele minime.În cazul în care calculatorul nu întrunește toate cerințele minime de sistem, Bitdefender nu va fi instalat sau nu va funcționa în mod corespunzător, determinând reducerea vitezei de funcționare și instabilitatea sistemului.Pentru o listă completă a cerințelor de sistem, consultați *„Cerințe de sistem”* (p. 3).
- Autentificați-vă pe calculator cu datele unui cont de administrator.
- Dezinstalați orice alt program similar de pe computer.Rularea simultană a două programe de securitate poate afecta funcționarea lor și poate provoca probleme majore ale sistemului.Windows Defender va fi dezactivat în timpul instalării.
- Dezactivați sau dezinstalați orice alt program firewall de pe calculator.Rularea simultană a două programe firewall poate afecta funcționarea lor și poate provoca probleme majore ale sistemului.Windows Firewall va fi dezactivat în timpul instalării.
- Se recomandă ca, în timpul instalării, computerul dumneavoastră să fie conectat la internet, chiar și atunci când realizați instalarea de pe un CD/DVD.Dacă sunt disponibile versiuni mai noi ale fișierelor aplicației decât cele incluse în pachetul de instalare, Bitdefender le va descărca și le va instala.

2. Cerințe de sistem

Puteți instala Bitdefender Internet Security 2013 doar pe calculatoare pe care rulează următoarele sisteme de operare:

- Windows XP cu Service Pack 3 (32 bit)
- Windows Vista cu Service Pack 2
- Windows 7 cu Service Pack 1
- Windows 8

Înainte de instalare, computerul dumneavoastră trebuie să îndeplinească cerințele minime de sistem.

Notă

Pentru a afla sistemul de operare Windows care rulează pe calculatorul dumneavoastră, precum și informații hardware, faceți clic-dreapta pe iconița **My Computer** de pe desktop și apoi selectați **Properties** din meniu.

2.1. Cerințe minime de sistem

- 1.8 GB spațiu liber disponibil pe hard disk (cel puțin 800 MB pe unitatea de sistem)
- Procesor de 800 MHz
- 1 GB de memorie (RAM)

2.2. Cerințe recomandate de sistem

- 2.8 GB spațiu liber disponibil pe hard disk (cel puțin 800 MB pe unitatea de sistem)
- Intel Core Duo (1.66 GHz) sau procesor echivalent
- RAM:
  - 1 GB pentru Windows XP
  - 1.5 GB pentru Windows Vista și Windows 7

2.3. Cerințe software

Pentru a putea utiliza Bitdefender și toate funcțiile sale, computerul dumneavoastră trebuie să întrunească următoarele cerințe software:

- Internet Explorer 7 sau o versiune mai recentă
- Mozilla Firefox 3.6 sau avansat
- Yahoo! Messenger 8.1 sau o versiune mai recentă
- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express și Windows Mail (pe sisteme de 32 bit)
- Mozilla Thunderbird 3.0.4
- .NET Framework 3.5 (instalat automat cu Bitdefender dacă nu există)

3. Scenarii de instalare

Instalare nouă

Nu există nicio versiune mai veche a Bitdefender instalată pe calculator. În acest caz, procedați conform instrucțiunilor din *„Instalarea produsului dumneavoastră Bitdefender”* (p. 5).

Instalarea actualizărilor

O versiune mai veche a fost deja instalată pe calculator și o actualizați la Bitdefender 2013. În acest caz, versiunea mai veche trebuie ștearsă înainte de instalare.

De exemplu, pentru a șterge Bitdefender 2012 înainte de instalare Bitdefender Internet Security 2013:

1. Urmați această cale din meniul de start Windows: **Start → All Programs → Bitdefender 2012 → Repair sau Remove**.
2. Selectați **Ștergere**.
3. Așteptați ca Bitdefender să finalizeze acțiunea pe care ați selectat-o. Această operațiune poate dura câteva minute.
4. Reporniți calculatorul pentru finalizarea procedurii.

Dacă nu ștergeți versiunea mai veche înainte de a începe instalarea Bitdefender Internet Security 2013, vi se va solicia să faceți acest lucru la începutul procesului de instalare. Urmați instrucțiunile pentru a finaliza ștergerea versiunii anterioare.

4. Instalarea produsului dumneavoastră Bitdefender

Puteți instala Bitdefender de pe CD-ul de instalare Bitdefender sau folosind fișierul de instalare web descărcat pe computerul dumneavoastră de pe site-ul Bitdefender sau de pe alte site-uri web autorizate (de exemplu, site-ul web al unui partener Bitdefender sau un magazin online).Puteți descărca fișierul de instalare de pe site-ul Bitdefender: http://www.bitdefender.ro/Downloads/.

Dacă achiziționați acoperiri pentru mai mult de un calculator (de exemplu, ați achiziționat Bitdefender Internet Security 2013 pentru 3 calculatoare), reluați procedura de instalare și înregistrați produsul cu codul de licență pe fiecare calculator.

- Pentru a instala Bitdefender de pe CD-ul de instalare, introduceți CD-ul în unitatea optică.În câteva momente se va afișa un ecran de întâmpinare. Urmați instrucțiunile pentru a începe instalarea.

  Notă

  Ecranul de întâmpinare oferă opțiunea de a copia pachetul de instalare de pe CD-ul de instalare pe un dispozitiv de stocare USB.Acest lucru este folositor în cazul în care doriți să instalați Bitdefender pe un computer care nu prezintă o unitate disc (de exemplu, pe un notebook).Introduceți dispozitivul de stocare în unitatea USB și apoi faceți clic pe **Copiere pe USB**.Apoi, mergeți la computerul fără unitate de disc, introduceți dispozitivul de stocare în drive-ul USB și faceți dublu-clic pe `runsetup.exe` din directorul în care ați salvat pachetul de instalare.

  Dacă nu apare ecranul de întâmpinare, folosiți Windows Explorer pentru a parcurge directorul rădăcină al CD-ului și faceți dublu clic pe fișierul `autorun.exe`.

- Pentru a instala Bitdefender folosind fișierul de instalare web descărcat pe calculator, localizați fișierul și faceți dublu-clic pe el.

Validarea instalării

Bitdefender va verifica mai întâi sistemul dvs, pentru a valida instalarea.

Dacă sistemul dumneavoastră nu îndeplinește cerințele minime pentru instalarea Bitdefender, veți fi informat cu privire la zonele ce necesită să fie îmbunătățite înainte să puteți continua.

Dacă este detectat un program antivirus necompatibil sau o versiune mai veche a Bitdefender, vi se va cere să le ștergeți de pe sistemul dumneavoastră.Vă rugăm să urmați instrucțiunile pentru a șterge software-ul din sistemul dumneavoastră, evitând astfel apariția problemelor pe viitor.Este posibil să fie nevoie să reporniți computerul pentru a finaliza dezinstalarea programelor antivirus detectate.

Pachetul de instalare Bitdefender Internet Security 2013 este actualizat constant. Dacă îl instalați de pe un CD/DVD, Bitdefender poate descărca versiunea cea mai

nouă a fișierelor în timpul instalării. Faceți clic pe **Da** când vi se solicită acest lucru pentru a permite Bitdefender să descarce fișierele, asigurându-vă că instalați cea mai recentă versiune a aplicației.

Notă
Descărcarea fișierelor de instalare poate dura foarte mult, cu precădere în cazul conexiunilor Internet mai lente.

După validarea instalării, se va afișa asistentul de configurare. Urmați pașii pentru instalarea Bitdefender Internet Security 2013.

Pasul 1 - Bun venit

Ecranul de întâmpinare vă permite să alegeți tipul de instalare pe care doriți să o efectuați.

Pentru o experiență de instalare fără probleme, nu trebuie decât să faceți clic pe butonul **Instalare**. Bitdefender va fi instalat în locația implicită cu setări implicite și veți trece direct la Pasul 3 al asistentului.

Dacă doriți să configurați setările de instalare, selectați **Diresc să personalizez instalarea** și apoi faceți clic pe **Instalare** pentru a trece la pasul următor.

În cadrul acestui pas se pot efectua două sarcini suplimentare:

- Vă rugăm să citiți Acordul de licență cu utilizatorul final înainte de a continua cu instalarea. Contractul de licență conține termenii și condițiile conform cărora puteți folosi Bitdefender Internet Security 2013.

  Dacă nu sunteți de acord cu acești termeni, închideți fereastra. Procesul de instalare va fi abandonat și veți ieși din fereastra de instalare.

- Activați transmiterea **Rapoartelor de utilizare anonime**. Prin activarea acestei opțiuni, sunt trimise rapoarte către serverele Bitdefender, conținând informații despre modul în care utilizați produsul. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să vă oferim produse și mai bune pe viitor. Rapoartele nu conțin date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scopuri comerciale.

Pasul 2 - Setări instalare personalizată

Notă
Acest pas apare numai dacă ați ales să personalizați instalarea la pasul anterior.

Sunt disponibile următoarele opțiuni:

Calea de instalare
În mod implicit, Bitdefender Internet Security 2013 va fi instalat în `C:\Program Files\Bitdefender\Bitdefender 2013`.Dacă doriți să schimbați calea

de instalare, faceți clic pe butonul **Modificare** și selectați directorul în care doriți să fie instalat Bitdefender.

Configurare setări proxy

Pentru înregistrarea produsului, Bitdefender Internet Security 2013 necesită acces la internet, descărcarea actualizărilor produsului și a celor de securitate, ale componentelor opțiunii de detecție in-cloud etc.Dacă folosiți o conexiune proxy în loc de o conexiune directă la internet trebuie să selectați această opțiune și să configurați setările proxy.

Setările pot fi importate din browser-ul implicit sau introduse manual.

Activare actualizare P2P

Puteți partaja fișierele produsului și semnăturile cu alți utilizatori Bitdefender.În acest mod, actualizările Bitdefender pot fi realizate mai rapid.Dacă nu doriți să activați această funcție, bifați căsuța corespunzătoare.

Notă

Nicio informație personală identificabilă nu va fi partajată dacă această funcție este activată.

Dacă doriți să reduceți impactul traficului din rețea asupra performanței sistemului în timpul actualizărilor, utilizați opțiunea de partajare a actualizărilor. Bitdefender utilizează porturile 8880 - 8889 pentru actualizarea peer-to-peer (P2P).

Faceți clic pe **Inszalare cu setări personalizate** pentru a vă confirma preferințele și a începe instalarea.

Pasul 3 - Instalare în curs de desfășurare

Așteptați până când instalarea este finalizată.În acest timp sunt afișate informații cu privire la progresul instalării.

Zonele critice ale sistemului dumneavoastră sunt scanate pentru identificarea virușilor, cele mai noi versiuni ale fișierelor aplicațiilor sunt descărcate și instalate, iar serviciile Bitdefender sunt pornite.Această etapă poate dura câteva minute.

Pasul 4 - Instalare finalizată

Este afișat rezumatul instalării. Dacă, în timpul instalării, este detectat și dezinstalat un program periculos, poate fi necesară o repornire a sistemului.

Puteți închide fereastra sau continua cu configurarea inițială a aplicației făcând clic pe **Inițiere**.

Pasul 5 - Înregistrați-vă produsul

Notă
Acest pas apare numai dacă ați selectat Inițiere la pasul anterior.

Pentru a finaliza înregistrarea produsului dumneavoastră, trebuie să introduceți un cod de licență.Este necesară o conexiune activă la internet.

Procedați în funcție de situația dumneavoastră:

- **Am achiziționat produsul**

  În acest caz, înregistrați produsul urmând acești pași:

  1. Selectați **Am achiziționat Bitdefender și doresc să îl înregistrez acum**.
  2. Introduceți seria de licență în câmpul corespunzător.

     Notă
     Puteți găsi seria dumneavoastră de înregistrare:
     - pe eticheta de la CD/DVD.
     - pe certificatul de înregistrare al produsului.
     - în e-mailul de achiziționare online.

  3. Faceți clic pe **Înregistrare**.

- **Doresc să evaluez Bitdefender**

  În acest caz, puteți utiliza produsul pe o perioadă de 30 de zile.Pentru a începe perioada de evaluare, selectați **Doresc să evaluez produsul**.

Faceți clic pe **Înainte**.

Pasul 6 - Configurarea comportamentului produsului

Bitdefender poate fi configurat pentru a vă administra automat setările de securitate permanent sau în anumite situații. Folosiți comutatoarele pentru a activa sau dezactiva opțiunea **Autopilot**, **Modul Laptop automat** și **Modul Joc automat**.

Activați funcția de Pilot automat pentru securitate complet silențioasă. După ce ați activat funcția Autopilot, Bitdefender ia toate deciziile legate de securitate pentru dumneavoastră și nu trebuie să configurați nicio setare. Pentru mai multe informații, consultați *„Autopilot”* (p. 16).

Dacă vă plac jocurile, activați Modul Joc automat și Bitdefender va detecta când lansați un joc și va intra în Modul Joc, modificând setările pentru a reduce la minimum impactul asupra performanțelor sistemului dumneavoastră. Pentru mai multe informații, consultați *„Mod jocuri”* (p. 17).

Pentru cei ce utilizează laptopuri, Modul Laptop automat va determina Bitdefender să treacă în modul laptop când detectează că laptopul funcționează cu energia de

la baterie, modificându-i setările astfel încât impactul asupra consumului bateriei să fie menținut la minimum. Pentru mai multe informații, consultați *„Mod laptop”* (p. 19).

Faceți clic pe **Înainte**.

Pasul 7 - Configurați filtrele de conectare

De aici puteți selecta filtrele de conexiune pentru activare.Există anumite filtre care vă asigură o protecție activă în timpul navigării pe Internet, atunci când sunteți conectat la o rețea.

Utilizați comutatoarele pentru activare/dezactivare:

- Antispam
- Firewall
- Aplicație contra programelor periculoase de pe Internet
- Antiphishing
- Antifraudă
- Asistență pentru căutare

Puteți activa sau dezactiva aceste filtre în orice moment după instalare direct din interfața Bitdefender. Pentru a obține cel mai bun nivel de protecție, se recomandă să activați toate filtrele.

Activați filtrul Antispam numai dacă folosiți un client de e-mail configurat să primească mesaje prin intermediul protocolului POP3.

Faceți clic pe **Înainte**.

Pasul 8 - Autentificare MyBitdefender

Este necesar cont MyBitdefender pentru a utiliza funcțiile online ale produsului. Pentru mai multe informații, consultați *„Contul MyBitdefender”* (p. 33).

Continuați în funcție de situația dumneavoastră.

Doresc să creez un cont MyBitdefender

Pentru a crea cu succes un cont MyBitdefender, urmați acești pași:

1. Selectați **Creare cont nou**.

   Va apărea o nouă fereastră.

2. Introduceți informațiile solicitate în câmpurile corespunzătoare.Informațiile furnizate aici vor rămâne confidențiale.

   - **E-mail** - introduceți adresa de e-mail.

- **Nume utilizator** - introduceți un nume de uilizator pentru contul dumneavoastră.
- **Parola** - introduceți o parolă pentru contul dumneavoastră. Parola trebuie să aibă cel puțin 6 caractere.
- **Confirmare parolă** - introduceți din nou parola.

Notă

După crearea contului, puteți folosi adresa de e-mail și parola furnizate pentru a vă autentifica în cont, la https://my.bitdefender.com.

3. Faceți clic pe **Creează**.
4. Înainte de a vă putea utiliza contul, trebuie să finalizați înregistrarea. Verificați-vă e-mail-ul și urmați instrucțiunile din e-mail-ul de confirmare trimis de Bitdefender.

Doresc să mă autentific prin intermediul contului de Facebook sau Google

Pentru a vă conecta cu contul de Facebook sau de Google, urmați pașii de mai jos:

1. Selectați serviciul pe care doriți să îl utilizați.Veți fi redirecționat către pagina de autentificare a acelui serviciu.
2. Urmați instrucțiunile oferite de serviciul selectat pentru a face legătura dintre contul dumneavoastră și Bitdefender.

Notă

Bitdefender nu are acces la informații confidențiale, precum parola contului pe care vă autentificați de obicei sau datele personale ale prietenilor și contactelor.

Am deja un cont MyBitdefender

Dacă v-ați conectat anterior la un cont din produsul dumneavoastră, Bitdefender îl va detecta și vă va solicita să introduceți parola pentru a vă autentifica în contul respectiv.

Dacă aveți deja un cont activ, însă Bitdefender nu îl detectează sau pur și simplu doriți să vă autentificați cu un alt cont, introduceți adresa e-mail și faceți clic pe **Autentificare la MyBitdefender**.

Amână pentru mai târziu

Dacă doriți să lăsați această sarcină pentru o dată ulterioară, faceți clic pe **Întreabă-mă mai târziu**. Nu uitați că trebuie să vă conectați la un cont pentru a utiliza funcțiile online ale produsului.

Primii pași

5. Informații de bază

Odată ce ați instalat Bitdefender Internet Security 2013, calculatorul dumneavoastră este protejat împotriva tuturor tipurilor de programe periculoase (cum ar fi virușii, programele spion și troienii) și amenințărilor de pe internet (cum ar fi piraților informatici, atacurile de tip phishing și mesajele spam).

Puteți activa funcția Autopilot pentru a vă bucura de securitate silențioasă și ca să nu mai fie nevoie de nicio intervenție din partea dumneavoastră pentru configurarea setărilor. Cu toate acestea, puteți profita de setările oferite de Bitdefender pentru a vă ajusta și îmbunătăți protecția.

Bitdefender va lua majoritatea deciziilor legate de securitate în locul dumneavoastră și va afișa rareori alerte pop-up.În fereastra Evenimente sunt disponibile acțiunile aplicate și informații cu privire la funcționarea programului. Pentru mai multe informații, consultați *„Evenimente”* (p. 15).

Din când în când, trebuie să deschideți Bitdefender și să remediați problemele existente. Este posibil să fie nevoie să configurați anumite componente ale Bitdefender sau să luați măsuri preventive pentru a vă proteja calculatorul și datele dumneavoastră.

Dacă nu ați înregistrat produsul, vă reamintim că trebuie să faceți acest lucru până la expirarea perioadei de evaluare. Pentru mai multe informații, consultați *„Înregistrarea Bitdefender”* (p. 31).

Pentru a folosi opțiunile online ale Bitdefender Internet Security 2013, este necesar să vă intrați în contul MyBitdefender. Pentru mai multe informații, consultați *„Contul MyBitdefender”* (p. 33).

Dacă vă confruntați cu probleme în utilizarea Bitdefender, accesați secțiunea *„Soluționarea problemelor frecvente”* (p. 131) pentru soluții posibile la cele mai frecvente probleme.În secțiunea „Cum să” (p. 40) veți găsi instrucțiuni pas cu pas de efectuare a sarcinilor obișnuite.

5.1. Deschiderea ferestrei Bitdefender

Pentru a accesa interfața principală a Bitdefender Internet Security 2013, folosiți meniul Start al Windows, urmând calea: **Start → All Programs → Bitdefender 2013 → Bitdefender Internet Security 2013** sau,mai rapid, faceți dublu clic pe pictograma Bitdefender din bara de sistem.

Pentru mai multe informații despre fereastra și pictograma Bitdefender de pe bara de sistem, consultați *„Interfața Bitdefender”* (p. 21).

5.2. Reparare probleme

Bitdefender utilizează un sistem de monitorizare a problemelor pentru a detecta și pentru a vă informa în legătură cu aspectele care pot afecta securitatea computerului și datelor dumneavoastră. În mod implicit, sunt monitorizate numai problemele considerate a fi foarte importante. Totuși, puteți configura sistemul după cum doriți, prin alegerea problemelor despre care doriți să primiți notificări.

Problemele depistate pot include setări de protecție importante care au fost dezactivate, precum și alte condiții care pot reprezenta un risc de securitate. Acestea sunt grupate în două categorii:

- **Probleme critice** - împiedicăBitdefender să vă protejeze împotriva softurilor periculoase sau reprezintă un risc de securitate major.
- **Probleme minore (necritice)** - vă pot afecta protecția în viitorul apropiat.

Pictograma Bitdefender de pe bara de sistem indică aspectele în curs de soluționare schimbându-și culoarea după cum urmează:

Culoarea roșie: Probleme critice afectează securitatea sistemului dumneavoastră. Acestea necesită atenția dvs imediat și trebuie remediate în cel mai scurt timp.

Culoarea galben: Probleme nu foarte importante afectează securitatea sistemului dumneavoastră. Ar trebui să verificați și să le remediați atunci când aveți timp.

De asemenea, dacă plasați cursorul mouse-ului peste iconiță, o fereastră pop-up va confirma existența unor probleme.

Când deschideți fereastra Bitdefender, zona de stare a securității de pe bara de instrumente superioară va indica numărul și tipul de probleme care afectează sistemul dvs.

5.2.1. Asistentul de remediere a tuturor problemelor

Pentru a remedia problemele detectate, urmați instrucțiunile asistentului **Remediază toate problemele**

1. Pentru a porni asistentul, aveți următoarele alternative:
   - Faceți clic-dreapta pe pictograma Bitdefender din bara de sistem și selectați **Remediază toate problemele**.În funcție de problemele detectate, pictograma este fie roșie (indicând probleme critice) fie galbenă (indicând probleme nu foarte grave).
   - Deschideți fereastra Bitdefender și faceți clic oriunde în interiorul zonei stării de securitate din partea superioară a barei de instrumente (de exemplu puteți face clic pe butonul **Remediere toate problemele**).

2. Puteți vizualiza problemele care afectează datele și securitatea computerului dumneavoastră.Toate problemele actuale sunt selectate pentru a fi remediate.

   Dacă nu doriți să soluționați o anumită problemă în acest moment, debifați căsuța corespunzătoare.Veți fi rugat să specificați intervalul de amânare pentru soluționarea problemei.Selectați opțiunea dorită din meniu și faceți clic pe **OK**.Pentru a opri monitorizarea respectivei categorii de probleme, selectați **Permanent**.

   Starea problemei se va schimba în **Amânare** și nu se va lua nicio măsură pentru remedierea problemei.

3. Pentru a rezolva problemele selectate, faceți clic pe **Start**. Unele probleme sunt remediate imediat. Pentru remedierea celorlalte, veți avea la dispoziție programe asistent separate.

Problemele pe care acest program asistent vă permite să le remediați pot fi grupate în următoarele categorii principale:

- **Setări de securitate dezactivate.** Aceste probleme sunt remediate pe loc, prin activarea setărilor de securitate în cauză.
- **Sarcini de securitate preventive pe care trebuie să le efectuați.** Când remediați astfel de probleme, un program asistent vă ajută să finalizați sarcina cu succes.

5.2.2. Configurarea alertelor de stare

Bitdefender vă poate informa când se detectează probleme în funcționarea următoarelor componente de program:

- Firewall
- Antispam
- Antivirus
- Actualizare
- Securitate browser

Puteți configura sistemul de alertare conform preferințelor dumneavoastră selectând problemele specifice despre care doriți să fiți informat. Urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **General**.
4. În fereastra **Setări generale**, selectați secțiunea **Avansat**.
5. Faceți clic pe link-ul **Configurare alerte de stare**.
6. Faceți clic pe selectoare pentru a activa sau a dezactiva alertele de stare, în funcție de preferințele dumneavoastră.

5.3. Evenimente

Bitdefender menține un jurnal detaliat al evenimentelor legate de activitatea sa pe computerul dumneavoastră. Ori de câte ori se întâmplă un lucru important pentru securitatea sistemului sau datelor dumneavoastră, se adaugă un nou mesaj la Evenimentele Bitdefender, ca și când ați primi un e-mail nou în Inbox-ul dumneavoastră.

Evenimentele reprezintă un instrument extrem de important pentru monitorizarea și gestionarea protecției Bitdefender.De exemplu, puteți verifica rapid dacă produsul a fost actualizat, dacă au fost detectate coduri sau aplicații periculoase pe calculatorul dumneavoastră etc.În plus, puteți lua măsuri suplimentare dacă este cazul sau puteți modifica măsurile luate prin intermediul Bitdefender.

Pentru a accesa jurnalul de Evenimente, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe **Evenimente** din bara de instrumente situată în partea de sus pentru a deschide fereastra **Prezentare evenimente**.

Mesajele sunt grupate conform modulului Bitdefender la a cărui activitate se referă:

- **Antivirus**
- **Antispam**
- **Control date**
- **Firewall**
- **Actualizare**
- **Safego**

Contoarele de evenimente sunt afișate pe interfața Bitdefender pentru a permite identificarea cu ușurință a zonelor cu evenimente excepționale. Acestea sunt pictograme care se afișează pe anumite module ce indică numărul de evenimente critice necitite asociate activității unui modul.

De exemplu, dacă există un eveniment critic necitit cu privire la activitatea modulului de Actualizare, pictograma  se afișează pe panoul Actualizare.

Un contor pe care se afișează numărul total de mesaje necitite din toate modulele se afișează pe butonul de Evenimente din fereastra principală.

Pentru fiecare categorie este disponibilă o listă de evenimente.Pentru a afla informații cu privire la un anumit eveniment din listă, faceți clic pe acesta. Detaliile despre eveniment vor fi afișate în partea inferioară a ferestrei.Fiecare eveniment este însoțit de următoarele informații: o scurtă descriere, acțiunea aplicată de Bitdefender în momentul producerii evenimentului și data și ora producerii acestuia.Pot fi setate diverse opțiuni prin intermediul cărora să fie aplicații și alte acțiuni, dacă este necesar.

Puteți filtra evenimentele în funcție de importanța acestora.Există trei tipuri de evenimente, fiecare marcat printr-o anumită pictogramă:

Evenimentele de tip **Informații** indică operațiile finalizate cu succes.

Evenimentele de tip **Avertizare** indică probleme care nu sunt de foarte mare importanță. Ar trebui să verificați și să le remediați atunci când aveți timp.

Evenimentele **critice** indică probleme critice. Acestea ar trebui verificate imediat.

Pentru a vă ajuta să gestionați cu ușurință evenimentele înregistrate, fiecare secțiune a ferestrei Evenimente oferă opțiuni de ștergere sau marcare ca citite a tuturor evenimentelor din secțiunea respectivă.

5.4. Autopilot

Pentru toți acei utilizatori care nu-și doresc nimic altceva de la soluția lor de securitate decât să fie protejați fără a fi deranjați, Bitdefender Internet Security 2013 a fost prevăzut cu modul integrat Autopilot.

Atunci când se află în modul Autopilot, Bitdefender aplică o configurație de securitate optimă și ia toate deciziile legate de securitate în locul dumneavoastră.Aceasta înseamnă că nu vor fi afișate ferestre pop-up, alerte și nu va fi necesar să configurați niciun fel de setări.

În modul Autopilot, Bitdefender remediază în mod automat problemele critice și activează și gestionează în mod silențios:

- Protecție antivirus, asigurată de funcția de scanare la accesare și scanare continuă.
- Protecție firewall.
- Protecția confidențialității asigurată de filtrele antiphishing și antimalware pentru activitatea dumneavoastră de navigare pe internet.
- Actualizări automate.

Pentru a activa sau dezactiva modul Autopilot, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Mod utilizator** / **Autopilot** din bara de instrumente situată în partea de sus. Atunci când butonul este în poziția Mod utilizator, funcția Autopilot este dezactivată.

Atunci când funcția Autopilot este activată, pictograma Bitdefender din bara de sistem va deveni .

Important
În cazul în care modificați vreo setare administrată de funcția Autopilot atunci când este activată, aceasta se va dezactiva în mod implicit.

Pentru a vizualiza istoricul acțiunilor efectuate de către Bitdefender cât timp a fost activată funcția Autopilot, deschideți fereastra Evenimente.

5.5. Modul pentru jocuri și Modul pentru laptop

Unele activități efectuate pe calculator, cum ar fi jocurile sau prezentările, necesită o viteză sporită de reacție și funcționare a sistemului, fără întreruperi.Când laptopul dvs se alimentează de la baterie, este recomandat să amânați operațiile cu consum mare de energie până când laptopul este conectat din nou la o priză.

Pentru a se adapta la aceste situații, Bitdefender Internet Security 2013 are două moduri de funcționare speciale:

- Mod jocuri
- Mod laptop

5.5.1. Mod jocuri

Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului.Următoarele setări se aplică atunci când Modul Joc este pe:

- Toate alertele și pop-upurile Bitdefender sunt dezactivate.
- Scanarea la accesare este setată la nivelul de protecție **Permisiv**.
- Funcția de Scanare automată este dezactivată.Scanarea automată detectează și folosește intervale de timp pentru a efectua scanări repetate ale întregului sistem, atunci când consumul de resurse de sistem scade sub un anumit prag.
- Firewallul Bitdefender este setat la modul normal (Modul Paranoid este dezactivat).Aceasta înseamnă că toate conexiunile noi (atât la intrare cât și la ieșire) sunt permise în mod automat, indiferent de portul și protocolul utilizat.
- Funcția de Actualizare automată este dezactivată.
- Bara de instrumente Bitdefender din browser-ul dumneavoastră este dezactivată atunci când vă jucați online, direct din browser-ul de internet.

Cât timp modul pentru jocuri este activat, puteți vedea litera G pe iconița Bitdefender.

Utilizarea modului pentru jocuri

În mod implicit, Bitdefender intră automat în modul pentru jocuri când porniți un joc din lista de jocuri cunoscute a Bitdefender sau când o aplicație ocupă întreg ecranul (fullscreen).Bitdefender va reveni automat la modul de funcționare normal atunci când închideți jocul sau când aplicația detectată iese din modul Ecran întreg.

Dacă doriți să activați modul pentru jocuri manual, folosiți una dintre următoarele metode:

- Faceți clic-dreapta pe icoana Bitdefender din bara de sistem și selectați **Activează modul pentru jocuri**.
- Activează folosind comanda rapidă de pe tastatură pentru Modul de joc. Apăsați simultan tastele `Ctrl+Shift+Alt+G` (combinația de taste implicită).

Important
Nu uitați să dezactivați modul pentru jocuri atunci când ați încheiat jocul. În acest scop, utilizați aceleași metode ca și la activarea sa.

Comandă rapidă de pe tastatură pentru Modul Joc

Pentru a seta și utiliza comanda rapidă de pe tastatură pentru intrarea în/ieșirea din modul de joc, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **General**.
4. În fereastra **Setări generale**, selectați secțiunea **General**.
5. Asigurați-vă că butonul de comandă rapidă de pe tastatură pentru modul de joc este activ.
6. Setați combinația de taste dorită:
   a. Combinația implicită este `Ctrl+Alt+Shift+G`.

      Bifați tastele speciale pe care doriți să le folosiți: tasta Control (`Ctrl`), tasta Shift (`Shift`) sau tasta Alternate (`Alt`).

   b. În câmpul editabil, tastați litera corespunzătoare tastei normale pe care doriți să o folosiți.

   De exemplu, dacă doriți să folosiți combinația de taste `Ctrl+Alt+D`, trebuie să bifați doar `Ctrl` și `Alt` și să tastați `D`.

Notă
Pentru a dezactiva combinația de taste, deselectați butonul **Tastă rapidă Mod pentru jocuri**.

Activarea sau dezactivarea modului automat de joc

Pentru a activa sau dezactiva modul automat de joc, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **General**.
4. În fereastra **Setări generale**, selectați secțiunea **General**.

5. Activați sau dezactivați modul de joc automat, făcând clic pe selectorul corespunzător.

5.5.2. Mod laptop

Modul Laptop se adresează utilizatorilor de laptop si notebook. Scopul acestuia este să minimizeze impactul pe care îl are Bitdefender asupra consumului bateriei atunci când aceste dispozitive funcționează pe baterie.Atunci când Bitdefender funcționează în modul Laptop, funcțiile de scanare automată și actualizare automată sunt dezactivate, deoarece necesită mai multe resurse de sistem și implicit sporesc consumul de energie.

Bitdefender detectează când laptopul dumneavoastră a trecut pe baterie și intră automat în modul pentru laptop.De asemenea, Bitdefender iese automat din modul pentru laptop, atunci când detectează că laptopul nu mai funcționează pe baterie.

Pentru a activa sau dezactiva modul automat de laptop, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **General**.
4. În fereastra **Setări generale**, selectați secțiunea **General**.
5. Activați sau dezactivați modul automat pentru laptop, făcând clic pe selectorul corespunzător.

Dacă Bitdefender nu este instalat pe un laptop, dezactivați modul automat pentru laptop.

5.6. Protecție cu parolă pentru setările Bitdefender

Dacă nu sunteți singura persoană cu drepturi administrative care folosește acest calculator, este recomandat să vă protejați setările Bitdefender cu o parolă.

Pentru a configura protecția prin parolă pentru setările Bitdefender, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **General**.
4. În fereastra **Setări generale**, selectați secțiunea **General**.
5. Activați protecția prin parolă apăsând butonul.
6. Faceți clic pe link-ul **Modificare parolă**.
7. Introduceți parola în cele două câmpuri și faceți clic pe **OK**.Parola trebuie să aibă cel puțin 8 caractere.

După ce ați setat o parolă, aceasta va trebuie introdusă de fiecare dată când cineva încearcă să modifice setările Bitdefender.

Important

Vă sfătuim să rețineți parola sau să o notați și să o păstrați într-un loc sigur.Dacă ați uitat parola, trebuie să reinstalați programul sau să contactați Bitdefender pentru asistență.

Pentru a elimina protecția prin parolă, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **General**.
4. În fereastra **Setări generale**, selectați secțiunea **General**.
5. Dezactivați protecția prin parolă făcând clic pe buton. Introduceți parola și faceți clic pe **OK**.

5.7. Rapoarte anonime privind consumul

În mod implicit, Bitdefender trimite rapoarte care conțin informații referitoare la modul de utilizare a acestuia pe serverele Bitdefender.Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să vă oferim produse și mai bune pe viitor.Rapoartele nu conțin date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scopuri comerciale.

În cazul în care nu mai doriți să trimiteți Rapoarte anonime privind consumul, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **General**.
4. În fereastra **Setări generale**, selectați secțiunea **Avansat**.
5. Faceți clic pe buton pentru a dezactiva rapoartele de utilizare Anonime.

6. Interfața Bitdefender

Bitdefender Internet Security 2013 îndeplinește deopotrivă cerințele persoanelor experimentate și pe cele ale începătorilor în utilizarea calculatorului. Interfața sa grafică este proiectată pentru a se potrivi fiecărei categorii de utilizatori.

Pentru a vizualiza starea produsului și pentru a efectua activități esențiale, pictograma brei de sistem a Bitdefender este disponibilă în permanență.

Ecranul principală vă oferă acces la informații importante de produs, la modulele programului și vă permite să efectuați sarcinile obișnuite. Din fereastra principală puteți accesa fereastra de setări pentru configurare detaliată și efectuarea sarcinilor administrative avansate și fereastra Evenimente pentru a vizualiza jurnalul detaliat al activității Bitdefender.

Dacă doriți să monitorizați în permanență informațiile de securitate esențiale și să aveți acces rapid la principalele setări, adăugați Widget-ul de securitate pe desktop.

6.1. Pictograma barei de sistem

Pentru a administra întregul produs mai rapid, puteți folosi iconița Bitdefender din bara de sistem.

Notă
Dacă folosiți Windows Vista sau Windows 7, este posibil ca pictograma Bitdefender să nu fie vizibilă întotdeauna. Pentru a vă asigura că această pictogramă este afișată permanent, urmați pașii de mai jos:

1. Faceți clic pe săgeata din colțul din dreapta jos al ecranului.
2. Faceți clic pe **Personalizare...** pentru a deschide fereastra Pictogramelor din zona notificărilor.
3. Selectați opțiunea **Afișare pictograme și notificări** pentru pictograma **Agent Bitdefender**.

Dacă faceți dublu-clic pe această iconiță, se va deschide fereastra Bitdefender. De asemenea, făcând clic-dreapta pe iconiță, un meniu contextual vă va oferi posibilitatea unei administrări rapide a Bitdefender.

- **Afișează** - deschide fereastra principală a Bitdefender.
- **Despre** - deschide o fereastră în care puteți vedea informații despre Bitdefender și unde puteți solicita asistență profesională în cazul unei probleme.
- **Remediază** - vă ajută să remediați problemele curente de securitate.Dacă opțiunea nu este disponibilă, nu există probleme care trebuie remediate.Pentru mai multe detalii, consultați *„Reparare probleme”* (p. 13).
- **Activează/Dezactivează Modul pentru jocuri** - activează/dezactivează modul pentru jocuri.

Pictogramă în bară

- **Ascundere/ Afișare widget de securitate** - activează / dezactivează widget-ul de securitate.
- **Actualizează acum** - inițiază o actualizare imediată.Puteți urmări starea actualizării pe panoul de actualizare din fereastra principală Bitdefender.

Iconița Bitdefender din bara de sistem vă informează despre problemele care vă afectează calculatorul sau despre funcționarea produsului, prin afișarea unui simbol special, după cum urmează:

Probleme critice afectează securitatea sistemului dumneavoastră. Acestea necesită atenția dvs imediat și trebuie remediate în cel mai scurt timp.

Probleme nu foarte importante afectează securitatea sistemului dumneavoastră.Ar trebui să verificați și să le remediați atunci când aveți timp.

Produsul funcționează în Modul pentru jocuri.

Funcția Autopilot a Bitdefender este activată.

Dacă Bitdefender nu funcționează, pictograma din bara de sistem apare pe un fundal gri: .Acest lucru se întâmplă de obicei când expiră licența. O altă cauză poate fi faptul că serviciile Bitdefender nu răspund sau că alte erori afectează funcționarea normală a Bitdefender.

6.2. Fereastra principală

Principala fereastră Bitdefender vă permite să realizați sarcini obișnuite, să remediați rapid probleme legate de securitate, să vizualizați informații referitoare la evenimente din cadrul funcționării produsului și să configurați setările produsului.Puteți accesa tot ce vă doriți făcând clic de câteva ori.

Fereastra este organizată în trei secțiuni principale:

Bara de instrumente din partea superioară

De aici puteți verifica starea securității computerului dumneavoastră și activitățile importante de acces.

Secțiunea panourilor

De aici puteți administra modulele principale Bitdefender.

Meniul derulant MyBitdefender din partea de sus a ferestrei vă permite să vă gestionați contul și să accesați funcționalitățile online ale produsului dumneavoastră folosind panoul de control.

În partea de jos a ferestrei, puteți găsi câteva link-uri utile. Aceste link-uri sunt disponibile și în ferestrele Evenimente și Setări.

Link	Descriere
Număr de zile rămase	Se afișează intervalul de timp rămas până la expirarea licenței curente.Faceți clic pe link pentru a deschide o fereastră în care veți putea vizualiza mai multe informații despre codul dumneavoastră de licență și vă veți putea înregistra produsul folosind un nou cod de licență.
Trimiteți feedback	Deschide o pagină web în browser-ul dumneavoastră, unde puteți completa un scurt chestionar privind experiența dumneavoastră în legătură cu utilizarea produsului.Ne bazăm pe feedback-ul primit de la dumneavoastră pentru a ne îmbunătăți în mod constant produsele Bitdefender.
Help and Support	Faceți clic pe acest link dacă aveți nevoie de ajutor cu Bitdefender. Se va afișa o nouă fereastră în care veți putea deschide secțiunea de ajutor a produsului, veți putea merge la Centrul de Asistență și veți putea contacta echipa de suport.
?	Adaugă semne de întrebare în diferite zone ale ferestrei Bitdefender pentru a vă ajuta să găsiți cu ușurință informații despre diferite elemente ale interfeței. Deplasați cursorul mouse-ului peste un marcaj pentru a vizualiza informații sumare despre elementul de lângă acesta.

6.2.1. Bara de instrumente din partea superioară

Bara de instrumente din partea superioară conține următoarele elemente:

- **Zona de stare a securității** din partea stângă a barei de instrumente vă informează dacă există probleme care afectează securitatea computerului dumneavoastră și vă ajută să le soluționați.

  Culoarea secțiunii stării de securitate se schimb în funcție de problemele detectate și, astfel, sunt afișate diferite mesaje:

  - **Secțiunea este colorată cu verde.** Nu există probleme de remediat.Calculatorul și datele dumneavoastră sunt protejate.

- **Secțiunea este colorată cu galben.** Probleme neimportante afectează securitatea sistemului dumneavoastră.Ar trebui să verificați și să le remediați atunci când aveți timp.
- **Secțiunea este colorată cu roșu.** Probleme critice afectează securitatea sistemului dumneavoastră.Ar trebui să vă ocupați de aceste probleme imediat.

Făcând clic pe **Vizualizare probleme** din centrul barei de instrumente sau oriunde în partea stângă a zonei de stare a securității, puteți accesa un program asistent care vă va ajuta să eliminați cu ușurință toate amenințările de pe computerul dumneavoastră.Pentru mai multe detalii, consultați *„Reparare probleme”* (p. 13).

- **Evenimente** vă permite să accesați un istoric detaliat al evenimentelor relevante care s-au produs în timpul funcționării produsului.Pentru mai multe detalii, consultați *„Evenimente”* (p. 15).
- Funcția **Setări** vă permite să accesați fereastra de setări, din care puteți configura setările produsului.Pentru mai multe detalii, consultați *„Fereastra Prezentare setări”* (p. 27).
- Butonul **Autopilot**/ **Mod utilizator** vă pemite să activați funcția Autopilot și să vă bucurați de securitate complet silențioasă. Pentru mai multe detalii, consultați *„Autopilot”* (p. 16).

6.2.2. Secțiunea panourilor

Din secțiunea panourilor puteți administra direct modulele Bitdefender.

Pentru a naviga printre panouri, folosiți cursorul de sub secțiunea panourilor sau săgețile localizate la dreapta și la stânga.

Fiecare panou de modul conține următoarele elemente:

- Denumirea modulului și un mesaj de stare.
- O pictogramă este disponibilă în colțul din dreapta sus la majoritatea panourilor. Dacă faceți clic pe aceasta, veți ajunge direct în fereastra de setări avansate a modulului respectiv.
- Pictograma modulului.

  Dacă există evenimente legate de activitatea unui modul pe care nu le-ați vizualizat încă, lângă pictograma modulului se va afișa un contor de evenimente. De exemplu, dacă există un eveniment necitit cu privire la activitatea modulului de Actualizare, pictograma se afișează pe panoul Actualizare. Faceți clic pe contor pentru a accesa direct fereastra de evenimente a modulului respectiv.
- Un buton care vă permite să efectuați activități importante care au legătură cu modulul.

- Un selector este disponibil pe anumite panouri, permițându-vă să activați sau să dezactivați o caracteristică importantă a modulului.

Puteți organiza panourile așa cum doriți, urmând pașii de mai jos:

1. Faceți clic pe din partea din stânga a barei de sub panouri pentru a deschide fereastra Prezentare module.
2. Trageți fiecare dintre panourile modulelor și fixați-le în căsuțele dorite pentru a le rearanja conform preferințelor dumneavoastră.
3. Faceți clic pe pentru a reveni la fereastra principală.

Panourile disponibile în această zonă sunt:

Antivirus

Protecția antivirus reprezintă fundația securității dumneavoastră. Bitdefender vă protejează în timp real și la cerere împotriva tuturor tipurilor de malware, precum viruși, troieni, programe de tip spyware, adware etc.

Din meniul Antivirus, puteți accesa cu ușurință sarcini de scanare importante.Faceți clic pe **Scanează acum** și selectați o sarcină din meniul vertical:

- QuickScan
- Scanare completă
- Scanare adaptabilă
- Vulnerabilități
- Mod de salvare

Selectorul de **Scanare automată** vă permite să activați sau să dezactivați funcția de scanare automată.

Pentru mai multe informații referitoare la activitățile de scanare și modul de configurare a protecției antivirus, consultați *„Protecție antivirus”* (p. 62).

Antispam

Modulul antispam al Bitdefender se asigură că nu intră e-mail-uri nedorite în directorul cu mesaje primite, filtrând traficul de mail POP3.

Protecția antispam nu este activată implicit. Componentele modulului sunt instalate la prima activare a acestui modul folosind butonul Antispam.

După activarea modulului, faceți clic pe **Gestionare** din panoul Antispam și selectați Prieteni sau Spammer-i din meniul vertical pentru a edita lista de adrese corespunzătoare.

Pentru mai multe informații referitoare la protecția antispam, consultați *„Antispam”* (p. 88).

Protecția datelor confidențiale

Modulul de control al datelor vă ajută să mențineți confidențialitatea datelor dumneavoastră personale importante.Atunci când navigați pe internet, vă protejează împotriva atacurilor de tip phishing, încercărilor de fraudă, scurgerilor de date personale și împotriva altor amenințări.

- **Ștergere definitivă fișiere** - lansează un program asistent care vă va permite să ștergeți definitiv fișierele.

Selectorul pentru Antiphishing vă permite să activați sau să dezactivați protecția antiphishing.

Pentru mai multe informații referitoare la modul de configurare Bitdefender pentru a vă proteja confidențialitatea, consultați *„Control date”* (p. 99).

Firewall

Firewall-ul vă protejează în timp ce sunteți conectat la rețele și la internet, filtrând toate tentativele de conectare.

Dacă selectați **Administrare adaptoare** din panoul Firewall, puteți configura setările de conectare generale pentru adaptoarele de rețea.

Selectorul pentru Firewall vă permite să activați sau să dezactivați protecție firewall.

Avertisment

Deoarece vă expune computerul unor conexiuni neautorizate, dezactivarea firewallului trebuie să fie doar o măsură temporară.Reactivați firewall-ul cât mai repede posibil.

Pentru mai multe informații cu privire la configurarea firewall-ului, consultați *„Firewall”* (p. 105).

Actualizare

Într-o lume în care infractorii cibernetici încearcă să descopere noi metode de a face rău, este esențial să vă mențineți actualizată soluția de securitate pentru a fi mereu cu un pas înainte acestora.

Implicit, Bitdefender verifică din oră în oră actualizările. Dacă doriți să dezactivați actualizările automate, folosiți selectorul **Actualizare automată** din panoul Actualizare.

Avertisment

Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați actualizarea automată pentru cât mai puțin timp posibil. Dacă nu este actualizat în mod regulat, Bitdefender nu va putea să vă protejeze împotriva ultimelor amenințări apărute.

Faceți clic pe butonul **Actualizează acum** din panou, pentru a iniția imediat o actualizare.

Pentru mai multe informații despre actualizările de configurare, consultați *„Actualizarea permanentă a Bitdefender”* (p. 36).

Safego

Pentru a vă asigura protecția în timp ce navigați în rețelele sociale, puteți accesa Safego, soluția de securitate a Bitdefender pentru rețele sociale direct din Bitdefender Internet Security 2013.

Faceți clic pe butonul **Gestionare** din panoul Safego și selectați o activitate din meniul derulant:

- **Activare pentru Facebook** folosind contul MyBitdefender. Dacă funcția Safego a fost deja activată, puteți accesa statisticile privind activitatea acesteia selectând din meniu **Vizualizare rapoarte pentru Facebook**.
- **Activare pentru Twitter** folosind contul MyBitdefender. Dacă funcția Safego a fost deja activată, puteți accesa statisticile privind activitatea acesteia selectând din meniu **Vizualizare rapoarte pentru Twitter**.

Pentru mai multe informații, consultați *„Protecție Safego pentru rețelele sociale”* (p. 125).

6.3. Fereastra Prezentare setări

Fereastra Prezentare setări vă oferă acces la setările avansate ale produsului dumneavoastră. Aici puteți configura Bitdefender în detaliu.

Selectați un modul pentru a configura setările și pentru a efectua sarcini de securitate sau administrative.Următoarea listă descrie pe scurt fiecare modul.

General

Vă permite să configurați setările generale ale produsului, precum parola pentru setări, Modul pentru jocuri, Modul laptop, setările pentru proxy și alertele de stare.

Antivirus

Vă permite să vă configurați protecția împotriva malware, să detectați și să remediați punctele vulnerabile ale sistemului dumneavoastră, să setați excepții de scanare și să gestionați fișierele aflate în carantină.

Antispam

Vă permite să țineți mesajele spam la distanță de căsuța dumneavoastră de mesaje și să configurați setările antispam în detaliu.

Control date

Vă permite să preveniți furtul de date și să vă protejați confidențialitatea în timp ce sunteți online. Configurați protecția pentru browser-ul dumneavoastră web, software-ul pentru mesageria instant, creați reguli de protecție a datelor și multe altele.

Firewall
Vă permite să configurați setările generale ale firewall-ului, regulile firewall-ului, detecția intruziunilor și activitatea de monitorizare a rețelei.

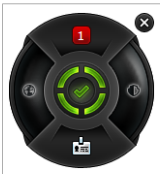
Actualizare
Vă permite să configurați în detaliu procesul de actualizare.

Pentru a reveni la fereastra principală, faceți clic pe din colțul din stânga sus al ferestrei.

6.4. Element de control de siguranță

Widget-ul de securitate reprezintă cea mai rapidă și ușoară metodă pentru monitorizarea și controlul Bitdefender Internet Security 2013. Adăugând acest widget la desktop, veți putea vizualiza informații importante și veți putea efectua sarcini cheie în orice moment:

- monitorizarea activității de scanare în timp real
- monitorizarea activității firewall-ului în timp real
- monitorizarea stării de securitate a sistemului dumneavoastră și remedierea problemelor existente
- vizualizarea notificărilor și acces la cele mai recente evenimente raportate de Bitdefender.
- acces printr-un singur clic la contul dumneavoastră MyBitdefender
- scanarea fișierelor și directoarelor prin tragerea și fixarea unuia sau a mai multor elemente în widget.



Element de control de siguranță

Starea generală de securitate a calculatorului dumneavoastră este afișată **în partea centrală** a widget-ului. Starea este indicată de culoarea și forma pictogramei afișate în această zonă.

Probleme critice afectează securitatea sistemului dumneavoastră.

Acestea necesită atenția dvs imediat și trebuie remediate în cel mai scurt timp. Faceți clic pe pictograma de stare pentru a începe remedierea problemelor raportate.


Probleme nu foarte importante afectează securitatea sistemului dumneavoastră. Ar trebui să verificați și să le remediați atunci când aveți timp. Faceți clic pe pictograma de stare pentru a începe remedierea problemelor raportate.


Sistemul dumneavoastră este protejat.


Atunci când o operațiune de scanare la cerere este în curs, se afișează această pictogramă animată.

Atunci când se raportează erori, faceți clic pe pictograma de stare pentru a lansa Asistentul de remediere a problemelor.

Butonul **din partea stângă** a widget-ului vă oferă acces direct la fereastra de setări pentru Firewall și, în plus, oferă o reprezentare grafică în timp real a activității firewall-ului. Atunci când pe acest buton apare o bară de culoare albastră, aceasta înseamnă că modulul firewall filtrează în mod activ conexiunile de rețea. Cu cât bara albastră este mai înaltă, cu atât mai intensă este activitatea acestui modul.

În **partea de sus** a widget-ului se afișează contorul evenimentelor necitite (numărul de evenimente nerezolvate raportate de Bitdefender, dacă există). Faceți clic pe contorul de evenimente, de exemplu  pentru un eveniment necitit, pentru a deschide fereastra Prezentare evenimente. Pentru mai multe informații, consultați *„Evenimente”* (p. 15).

Butonul **din partea dreaptă** a widget-ului vă oferă acces direct la fereastra de setări pentru Antivirus și, în plus, oferă o reprezentare grafică în timp real a activității de scanare. Atunci când se afișează o bară albastră pe acest buton, aceasta indică faptul că există sarcini de scanare în curs în timp real. Cu cât bara albastră este mai înaltă, cu atât mai intensă este activitatea acestui modul.

Butonul **din partea de jos** a widget-ului lansează panoul de control MyBitdefender într-o fereastră de browser web. Pentru mai multe informații, consultați *„Contul MyBitdefender”* (p. 33).

6.4.1. Scanarea fișierelor și directoarelor

Puteți utiliza Widget-ul de securitate pentru a scana rapid fișiere și directoare.Trageți și fixați orice fișier sau director pe care doriți să-l scanați direct în **Widget-ul de securitate**.

Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.Opțiunile de scanare sunt pre-configurate pentru a obține rata maximă de detecție și nu pot fi modificate.Atunci când se detectează fișiere infectate, Bitdefender va încerca să le curețe (să elimine codul malware). Dacă această acțiune de curățare eșuează, asistentul de scanare Antivirus vă va permite să specificați alte acțiuni pentru a fi aplicate în cazul fișierelor infectate.

6.4.2. Ascundere / afișare Widget de securitate

Dacă nu mai doriți ca widget-ul să fie vizibil, faceți clic pe .

Pentru a reafișa Widget-ul de securitate, urmați pașii de mai jos:

1. Faceți clic dreapta pe pictograma Bitdefender din bara de sistem.
2. Faceți clic pe **Afișare widget de securitate** din meniul contextual afișat.

7. Înregistrarea Bitdefender

Pentru a fi protejați de Bitdefender, trebuie să vă înregistrați produsul cu un cod de licență.Seria de înregistrare precizează pentru cât timp aveți dreptul de a utiliza produsul.Imediat după expirarea seriei de înregistrare, Bitdefender se va opri din funcționare și nu vă va mai proteja calculatorul.

Este recomandat să achiziționați o serie de înregistrare sau să vă reînnoiți licența cu câteva zile înainte de expirarea seriei actuale de înregistrare.Pentru mai multe informații, consultați *„Achiziționarea sau reînnoirea seriilor de licență”* (p. 32).În cazul în care utilizați o versiune de încercare a Bitdefender, trebuie să o înregistrați cu o serie de licență dacă doriți să utilizați produsul în continuare, după expirarea perioadei de evaluare.

7.1. Specificarea seriei de licență

Dacă, în timpul instalării, selectați să evaluați produsul, puteți folosi produsul pe o perioadă de încercare de 30 de zile.Pentru a folosi în continuare Bitdefender după expirarea perioadei de încercare, trebuie să înregistrați produsul cu o serie de licență.

Un link cu numărul de zile rămase în licența dumneavoastră se afișează în partea de jos a ferestrei Bitdefender. Faceți clic pe acest link pentru a deschide fereastra de înregistrare.

Puteți vedea starea înregistrării produsului dumneavoastră Bitdefender, seria actuală de înregistrare și câte zile au mai rămas până la expirarea licenței.

Pentru a înregistra Bitdefender Internet Security 2013:

1. Introduceți seria de înregistrare în câmpul editabil.

Notă

Puteți găsi seria dumneavoastră de înregistrare:

- pe eticheta de pe CD.
- pe certificatul de înregistrare al produsului.
- în e-mailul de achiziționare online.

Dacă nu aveți o serie de licență pentru Bitdefender faceți clic pe link-ul specificat în fereastră pentru a deschide o pagină web, de pe care puteți achiziționa o serie.

2. Faceți clic pe **Înregistrare**.

Chiar și după ce cumpărați un cod de licență, până la finalizarea înregistrării produsului cu codul, Bitdefender Internet Security 2013 va fi în continuare afișat ca versiune de încercare.

7.2. Achiziționarea sau reînnoirea seriilor de licență

Dacă perioada de evaluare se va încheia în curând, trebuie să achiziționați o serie de înregistrare și să vă înregistrați produsul.În mod similar, dacă seria de înregistrare actuală va expira în curând, trebuie să vă reînnoiți licența.

Bitdefender vă va avertiza atunci când se apropie data de expirare a licenței dumneavoastră actuale. Urmați instrucțiunile din mesajul de avertizare pentru a achiziționa o nouă licență.

Puteți vizita o pagină web de unde puteți achiziționa oricând o serie de licență, urmând pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe link-ul cu numărul de zile rămase din licența dumneavoastră, din partea de jos a ferestrei Bitdefender, pentru a deschide fereastra de înregistrare a produsului.
3. Faceți clic pe **Nu aveți o serie de licență? Cumpărați una acum!**
4. Se va deschide o pagină de web pe browser-ul dumneavoastră în care puteți achiziționa o serie de licență Bitdefender.

8. Contul MyBitdefender

Caracteristicile online ale produsului și serviciile Bitdefender suplimentare sunt disponibile exclusiv prin MyBitdefender. Trebuie să conectați calculatorul la MyBitdefender autentificându-vă direct din Bitdefender Internet Security 2013 pentru a putea efectua următoarele operațiuni:

- Notați-vă seria de licență, pentru în cazul în care se întâmplă să o pierdeți.
- Configurarea setărilor de Control Parental pentru conturile de Windows ale copiiilor dumneavoastră și monitorizarea activității acestora de la distanță.
- Protecție pentru conturile dumneavoastră de Facebook și Twitter prin intermediul Safego.
- Gestionarea Bitdefender Internet Security 2013 de la distanță.

Multiple soluții de securitate Bitdefender pentru PC-uri și alte platforme se integrează cu MyBitdefender. Puteți gestiona securitatea tuturor dispozitivelor conectate la contul dumneavoastră folosind un singur panou de control centralizat.

Contul dumneavoastră MyBitdefender poate fi accesat de la orice dispozitiv conectat la Internet la https://my.bitdefender.com.

De asemenea, puteți accesa și gestiona contul dumneavoastră direct din interfața produsului:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe **MyBitdefender** în partea de sus a ferestrei și selectați o opțiune din meniul derulant:
   - **Setări cont**

     Autentificați-vă, creați-vă un cont nou, configurați setările MyBitdefender.
   - **Dashboard**

     Lansați panoul de control MyBitdefender într-un browser web.
   - **Control Parental**

     Monitorizarea și controlul utilizării calculatorului de către copilul dumneavoastră

8.1. Conectarea calculatorului la MyBitdefender

Pentru a vă conecta calculatorul la contul MyBitdefender, trebuie să vă autentificați direct din Bitdefender Internet Security 2013. Până la finalizarea operațiunii de conectare a calculatorului la MyBitdefender, vi se va solicita să vă autentificați în MyBitdefender de fiecare dată când doriți să folosiți o funcționalitate care necesită existența unui astfel de cont.

Pentru a deschide fereastra MyBitdefender din care puteți crea un cont sau în care vă puteți autentifica, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe **MyBitdefender** în partea de sus a ferestrei și apoi selectați **Setări cont** din meniul derulant.

Dacă v-ați autentificat deja, se va afișa contul curent. Faceți clic pe **Mergeți la MyBitdefender** pentru a accesa panoul de control. Pentru a modifica contul asociat la calculator, selectați opțiunea de autentificare în alt cont.

Dacă nu v-ați autentificat în niciun cont, procedați în funcție de situație.

Doresc să creez un cont MyBitdefender

Pentru a crea cu succes un cont MyBitdefender, urmați acești pași:

1. Selectați **Creează cont nou**.

   Va apărea o nouă fereastră.

2. Introduceți informațiile solicitate în câmpurile corespunzătoare.Informațiile furnizate aici vor rămâne confidențiale.

   - **E-mail** - introduceți adresa de e-mail.
   - **Nume utilizator** - introduceți un nume de uilizator pentru contul dumneavoastră.
   - **Parola** - introduceți o parolă pentru contul dumneavoastră.Parola trebuie să aibă cel puțin 6 caractere.
   - **Confirmare parolă** - introduceți din nou parola.

3. Faceți clic pe **Creează**.
4. Înainte de a vă putea utiliza contul, trebuie să finalizați înregistrarea. Verificați-vă e-mail-ul și urmați instrucțiunile din e-mail-ul de confirmare trimis de Bitdefender.

Doresc să mă autentific prin intermediul contului de Facebook sau Google

Pentru a vă conecta cu contul de Facebook sau de Google, urmați pașii de mai jos:

1. Faceți clic pe pictograma serviciului pe care doriți să-l folosiți pentru a vă autentifica.Veți fi redirecționat către pagina de autentificare a acelui serviciu.
2. Urmați instrucțiunile oferite de serviciul selectat pentru a face legătura dintre contul dumneavoastră și Bitdefender.

Notă

Bitdefender nu are acces la informații confidențiale, precum parola contului pe care vă autentificați de obicei sau datele personale ale prietenilor și contactelor.

Am deja un cont MyBitdefender

Dacă aveți deja un cont, dar nu l-ați accesat încă, urmați pașii de mai jos pentru autentificare:

1. Introduceți adresa de e-mail și parola contului dvs în câmpurile corespunzătoare.

Notă
Dacă v-ați uitat parola, faceți clic pe **V-ați uitat parola** și urmați instrucțiunile pentru a o recupera.

2. Faceți clic pe **Autentificare în MyBitdefender**.

Odată ce calculatorul a fost asociat unui cont, puteți folosi adresa de e-mail și parola furnizate pentru a vă autentifica accesând https://my.bitdefender.com.

De asemenea, vă puteți accesa contul direct din Bitdefender Internet Security 2013 folosind meniul derulant din partea de sus a ferestrei.

9. Actualizarea permanentă a Bitdefender

Zi de zi sunt descoperite și identificate noi programe virale. De aceea, este foarte importantă actualizarea Bitdefender cu ultimele semnături de aplicații malițioase.

Dacă sunteți conectat la Internet, prin bandă largă sau ADSL, Bitdefender se ocupă singur de actualizări. În mod implicit, caută actualizări când deschideți calculatorul și apoi la fiecare **oră**. În cazul în care este detectată o actualizare, aceasta este descărcată și instalată automat pe computerul dumneavoastră.

Procesul de actualizare este realizat progresiv, ceea ce inseamna ca fisierele care trebuie actualizate sunt inlocuite unul cate unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

Important

Mențineți funcția Actualizare automată activată pentru a fi protejat împotriva celor mai noi amenințări.

În anumite cazuri este necesară intervenția dumneavoastră pentru ca protecția oferită de Bitdefender să fie actualizată:

- Dacă computerul dumneavoastră este conectat la internet printr-un server proxy, trebuie să configurați setările proxy, după cum se specifică în *„Cum pot configura Bitdefender să utilizeze o conexiune la internet de tip proxy?”* (p. 56).
- Dacă nu beneficiați de conexiune la internet, puteți efectua actualizarea Bitdefender manual, după cum este specificat în *„Calculatorul meu nu este conectat la Internet. Cum actualizez Bitdefender?”* (p. 137).Fișierul de actualizare manuală este lansat o dată pe săptămână.
- În timpul descărcării actualizărilor pe o conexiune lentă de internet pot apărea erori. Pentru a afla cum să procedați în cazul unor astfel de erori, vă rugăm să consultați *„Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet”* (p. 137).
- Dacă vă conectați la Internet prin dial-up, atunci este recomandat să actualizați manual Bitdefender în mod regulat.Pentru mai multe informații, consultați *„Efectuarea unei actualizări”* (p. 37).

9.1. Cum verificați dacă Bitdefender este actualizat

Pentru a verifica dacă protecția oferită de produsul dumneavoastră Bitdefender este actualizată, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Actualizare**, căutați ora ultimei actualizări în denumirea panoului.

Pentru mai multe informații despre cele mai recente actualizări, verificați evenimentele privind actualizările:

1. În fereastra principală, faceți clic pe **Evenimente** din partea superioară a barei de instrumente.
2. În fereastra **Prezentare evenimente**, faceți clic pe **Actualizare**.

Puteți afla atunci când anume au fost inițiate actualizări, precum și informații despre acestea (dacă au fost finalizate cu succes, dacă este necesară o repornire pentru a finaliza instalarea).Dacă este necesar, reporniți sistemul cât mai curând posibil.

9.2. Efectuarea unei actualizări

Pentru efectuarea actualizărilor este necesară existența unei conexiuni la internet.

Pentru a iniția o actualizare, aplicați una dintre metodele de mai jos:

- Deschideți fereastra Bitdefender și faceți clic pe **Actualizează acum** în panoul **Actualizare** .
- Faceți clic dreapta pe pictograma Bitdefender din bara de sistem și selectați **Actualizează acum**.

Modulul Actualizare se va conecta la serverul de actualizare al Bitdefender și va căuta noi actualizări.În cazul în care este detectată o actualizare, în funcție de setările de actualizare, vi se va cere fie să confirmați actualizarea, fie aceasta va fi realizată automat.

Important
Poate fi necesar ca după realizarea unei actualizări să reporniți calculatorul. Vă recomandăm să faceți acest lucru cât mai repede cu putință.

9.3. Activarea sau dezactivarea actualizării automate

Pentru a dezactiva funcția de actualizare automată, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Actualizare**, faceți clic pe butonul **Actualizare automată**.
3. Se va deschide o fereastră de avertizare.Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării actualizarii automate. Puteți dezactiva actualizarea automată pentru 5, 15 sau 30 minute, pentru o oră, permanent sau doar până la repornirea sistemului.

Avertisment
Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați actualizarea automată pentru cât mai puțin timp posibil. Dacă nu este actualizat în mod regulat, Bitdefender nu va putea să vă protejeze împotriva ultimelor amenințări apărute.

9.4. Ajustarea setărilor de actualizare

Actualizările pot fi realizate din rețeaua locală, de pe Internet, direct sau printr-un server proxy.Implicit, Bitdefender va căuta actualizări la fiecare oră, pe Internet, și va instala actualizările disponibile fără a vă mai avertiza.

Setările de actualizare implicite sunt potrivite pentru majoritatea utilizatorilor, și, în mod normal, nu este nevoie să le modificați.

Pentru ajustarea setărilor de actualizare, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Actualizare**.
4. În fereastra **Setări actualizare**, ajustați setările conform preferințelor dumneavoastră.

Locație actualizare

Produsul Bitdefender este configurat să efectueze online actualizări de pe serverele de actualizare ale Bitdefender.Locația de actualizare este `http://upgrade.bitdefender.com`, o adresă de internet generică, ce este redirecționată automat către cel mai apropiat server de actualizare al Bitdefender din regiunea dumneavoastră.

Nu schimbați locația pentru actualizări decât dacă sunteți sfătuit de un reprezentant al Bitdefender sau de administratorul rețelei (dacă sunteți conectat la o rețea de birou) să faceți acest lucru.

Puteți reveni la locația de actualizare online generică făcând clic pe **Implicit**.

Reguli de procesare a actualizării

Puteți alege una dintre cele trei metode de mai jos pentru a descărca și instala actualizări:

- **Actualizare discretă** - Bitdefender descarcă și realizează actualizarea automat.
- **Anunță înainte de descărcare** - de fiecare dată când o actualizare este disponibilă, veți fi anunțat înainte de a o descărca.
- **Anunța înainte de instalare** - de fiecare dată când o actualizare a fost descărcată, veți fi întrebat înainte de a o instala.

Anumite actualizări necesită o repornire a computerului pentru a finaliza procesul de instalare.Implicit, dacă o actualizare necesită repornirea computerului, Bitdefender va continua să funcționeze cu fișierele vechi până în momentul în care utilizatorul repornește computerul. În acest fel, procesul de actualizare a Bitdefender nu interferează cu operațiile utilizatorului.

Dacă doriți să fiți notificat în momentul în care este necesară o repornire în urma unei actualizări, dezactivați opțiunea **Amânare repornire**, făcând clic pe comutatorul corespunzător.

Actualizări P2P

Pe lângă mecanismul obișnuit de actualizare, Bitdefender folosește, de asemenea, un sistem inteligent de partajare a actualizărilor bazat pe un protocol peer-to-peer prin intermediul căruia distribuie utilizatorilor Bitdefender actualizările semnăturilor programelor periculoase.

Puteți activa sau dezactiva opțiunile de actualizare P2P cu ajutorul comutatoarelor corespunzătoare.

Utilizare actualizare de sistem P2P

Activați această opțiune pentru a descărca actualizări de semnături malware de la alți utilizatori Bitdefender folosind sistemul de actualizare P2P.Bitdefender utilizează porturile 8880 - 8889 pentru actualizarea peer-to-peer (P2P).

Distribuire fișiere Bitdefender

Pentru a partaja cele mai recente semnături malware disponibile pe computerul dumneavoastră cu alți utilizatori Bitdefender, activați această opțiune.

Cum să

10. Instalare

10.1. Cum instalez Bitdefender pe un al doilea calculator?

Dacă ați cumpărat o licență pentru mai multe calculatoare, puteți folosi același cod de licență pentru a înregistra și celelalte calculatoare.

Pentru a instala Bitdefender în mod corect pe un al doilea calculator, urmați pașii de mai jos:

1. Instalați Bitdefender de pe CD/ DVD sau, dacă ați achiziționat produsul online, folosiți fișierul de instalare furnizat în e-mail-ul de confirmare, urmând aceiași pași de instalare.
2. Când apare fereastra de înregistrare, introduceți codul de licență și apoi faceți clic pe **Înregistrare**.
3. La următorul pas, aveți posibilitatea de a vă autentifica în contul dumneavoastră MyBitdefender sau de a crea un nou cont MyBitdefender.

   De asemenea, puteți alege să creați mai târziu contul MyBitdefender.
4. Așteptați până la finalizarea procesului de instalare și închideți fereastra.

10.2. Când este cazul să reinstalez Bitdefender?

Există anumite cazuri în care poate fi necesar să reinstalați produsul dumneavoastră Bitdefender.

Printre cazurile care ar putea necesita reinstalarea Bitdefender se numără următoarele:

- ați reinstalat sistemul de operare
- ați achiziționat un nou computer
- doriți să schimbați limba de afișare a interfeței Bitdefender

Pentru a reinstala Bitdefender puteți folosi CD-ul de instalare pe care l-ați achiziționat sau puteți descărca o nouă versiune de pe site-ul web Bitdefender.

În timpul instalării, vi se va solicita să înregistrați seria de licență pentru produsul dumneavoastră.

Dacă nu puteți găsi seria de licență, vă puteți autentifica în cadrul https://my.bitdefender.com pentru a o recupera. Introduceți adresa de e-mail și parola contului dvs în câmpurile corespunzătoare.

10.3. Cum trec de la Bitdefender 2013 la un alt produs?

Puteți trece cu ușurință de la un produs Bitdefender 2013 la un altul.

Cele trei produse Bitdefender 2013 pe care le puteți instala pe sistemul dumneavoastră sunt următoarele:

- Bitdefender Antivirus Plus 2013
- Bitdefender Internet Security 2013
- Bitdefender Total Security 2013

Dacă doriți să instalați pe sistemul dumneavoastră un alt produs Bitdefender 2013 decât cel cumpărat, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Un link cu numărul de zile rămase în licența dumneavoastră se afișează în partea de jos a ferestrei Bitdefender. Faceți clic pe acest link pentru a deschide fereastra de înregistrare.
3. Introduceți seria de înregistrare și faceți clic pe **Înregistrare**.
4. Bitdefender vă va informa că respectiva serie de înregistrare este destinată unui alt produs și vă va oferi opțiunea de a-l instala. Faceți clic pe linkul corespunzător și urmați procedura pentru a efectua instalarea.

11. Înregistrare

11.1. Ce produs Bitdefender folosesc?

Pentru a afla ce program Bitdefender ați instalat, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În partea superioară a ferestrei, ar trebui să vedeți afișată una dintre următoarele denumiri de produse:
   - Bitdefender Antivirus Plus 2013
   - Bitdefender Internet Security 2013
   - Bitdefender Total Security 2013

11.2. Cum pot înregistra o versiune de încercare?

Dacă ați instalat o versiune de încercare, o puteți folosi doar pentru o anumită perioadă. Pentru a folosi în continuare Bitdefender după expirarea perioadei de încercare, trebuie să înregistrați produsul cu o serie de licență.

Pentru a înregistra Bitdefender, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Un link cu numărul de zile rămase în licența dumneavoastră se afișează în partea de jos a ferestrei Bitdefender. Faceți clic pe acest link pentru a deschide fereastra de înregistrare.
3. Introduceți seria de înregistrare și faceți clic pe **Înregistrare**.

   Dacă nu aveți o serie de licență, faceți clic pe link-ul specificat în fereastră pentru a vizita pagina web de unde puteți achiziționa o serie.
4. Așteptați până la finalizarea procesului de înregistrare și închideți fereastra.

11.3. Când expiră protecția oferită de produsul meu Bitdefender?

Pentru a afla numărul de zile rămase până la expirarea seriei de licență, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Un link cu numărul de zile rămase în licența dumneavoastră se afișează în partea de jos a ferestrei Bitdefender.
3. Pentru informații suplimentare, faceți clic pe link pentru a deschide fereastra de înregistrare.

4. În fereastra **Înregistrare produs**, puteți efectua următoarele:
   - Vizualizați codul de licență folosit în prezent
   - Înregistrați produsul folosind un alt cod de licență
   - Cumpărați o nouă licență

11.4. Cum înregistrez Bitdefender fără a fi conectat la internet?

Dacă tocmai ați achiziționat Bitdefender dar nu aveți acces la o conexiune la internet, puteți înregistra Bitdefender offline.

Pentru a vă înregistra Bitdefender cu seria de licență, urmați pașii de mai jos:

1. Accesați un computer conectat la internet. De exemplu, puteți utiliza computerul unui prieten sau un computer dintr-o locație publică.
2. Mergeți la https://my.bitdefender.com pentru a crea un cont MyBitdefender.
3. Vă conectați la contul dumneavoastră.
4. Faceți clic pe numele de utilizator din partea de sus și selectați **Produse** din meniul derulant.
5. Faceți clic pe **Înregistrare offline**.
6. Introduceți seria de licență pe care ați achiziționat-o.
7. Faceți clic pe **Trimitere** pentru a obține un cod de autorizare.

   Important
   Notați-vă codul de autorizare.

8. Reveniți la computer cu codul de autorizare.
9. Deschideți fereastra Bitdefender.
10. Un link cu numărul de zile rămase în licența dumneavoastră se afișează în partea de jos a ferestrei Bitdefender. Faceți clic pe acest link pentru a deschide fereastra de înregistrare.
11. Introduceți codul de autorizare în câmpul corespunzător și faceți clic pe **Înregistrare**.
12. Așteptați până la finalizarea procesului de înregistrare.

11.5. Cum îmi reînnoiesc protecția Bitdefender?

Atunci când protecția Bitdefender se apropie de data expirării, trebuie să vă reînnoiți seria de licența.

- Urmați acești pași pentru a vizita un site web în care vă puteți reînnoi seria de licență Bitdefender:

1. Deschideți fereastra Bitdefender.
2. Un link cu numărul de zile rămase în licența dumneavoastră se afișează în partea de jos a ferestrei Bitdefender. Faceți clic pe acest link pentru a deschide fereastra de înregistrare.
3. Faceți clic pe **Nu aveți o serie de licență? Cumpărați una acum!**
4. Se va deschide o pagină de web pe browser-ul dumneavoastră în care puteți achiziționa o serie de licență Bitdefender.

Notă
Drept alternativă, puteți contacta retailer-ul de la care ați achiziționat Bitdefender.

- Urmați acești pași pentru a vă înregistra Bitdefender cu noua serie de licență:

1. Deschideți fereastra Bitdefender.
2. Un link cu numărul de zile rămase în licența dumneavoastră se afișează în partea de jos a ferestrei Bitdefender. Faceți clic pe acest link pentru a deschide fereastra de înregistrare.
3. Introduceți seria de înregistrare și faceți clic pe **Înregistrare**.
4. Așteptați până la finalizarea procesului de înregistrare și închideți fereastra.

Pentru mai multe informații și asistență puteți contacta Bitdefender, după cum este descris în secțiunea *„Solicitarea ajutorului”* (p. 156).

12. Scanarea cu Bitdefender

12.1. Cum scanez un fișier sau un director?

Cea mai ușoară și recomandată metodă de a scana un fișier sau un director este de a face clic dreapta pe un obiect pe care doriți să-l scanați, alegeți Bitdefender și selectați **Scanează cu Bitdefender** din meniu. Pentru finalizarea procesului de scanare, urmați pașii asistentului de scanare antivirus. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate.

Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

Iată câteva situații în care este recomandată folosirea acestei metode de scanare:

- Suspectați un anumit fișier sau director că este infectat.
- Atunci când descărcați de pe Internet fișiere care credeți că ar putea fi periculoase.
- Scanați un director comun din rețea înainte de a copia fișiere din acesta pe calculatorul dumneavoastră.

12.2. Cum îmi scanez sistemul?

Pentru a efectua o scanare completă a sistemului, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antivirus**, faceți clic pe **Scanează acum** și selectați **Scanare sistem** din meniul derulant.
3. Urmați programul asistent de scanare pentru a finaliza scanarea. Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate. Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora. Pentru mai multe informații, consultați *„Programul asistent de scanare”* (p. 73).

12.3. Cum creez o activitate de scanare personalizată?

Dacă doriți să scanați anumite locații de pe computer sau pentru a configura opțiunile de scanare, puteți configura și rula o sarcină de scanare personalizată.

Pentru a crea o activitate de scanare personalizată, procedați după cum urmează:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antivirus**, faceți clic pe **Scanează acum** și selectați **Scanare personalizată** din meniul derulant.
3. Faceți clic pe **Adaugă obiect** pentru a selecta fișierele sau directoarele ce vor fi scanate.

4. Dacă doriți să configurați în detaliu opțiunile de scanare, faceți clic pe **Opțiuni scanare**.

   Puteți configura ușor opțiunile de scanare reglând nivelul de scanare. Trageți cursorul deasupra scalei pentru a seta nivelul de scanare dorit.

   De asemenea, aveți posibilitatea de a închide computerul după finalizarea scanării în cazul în care nu a fost detectată nicio amenințare. Rețineți faptul că acesta va fi modul implicit de reacție, de fiecare dată când executați această activitate.

5. Faceți clic pe **Pornire scanare** și urmați instrucțiunile asistentului de scanare antivirus pentru a finaliza operația de scanare. După finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.

6. Dacă doriți să salvați activitatea de scanare pentru a o utiliza pe viitor, deschideți din nou fereastra de configurare.

7. Localizați scanarea pe care tocmai ați executat-o în lista **Scanări rapide**.

8. Puneți cursorul mouse-ului pe numele scanării, apoi faceți clic pe pictograma pentru a adăuga scanarea la lista de scanări favorite.

9. Introduceți un nume sugestiv pentru scanare.

12.4. Cum exclud un director de la procesul de scanare?

Bitdefender permite excluderea anumitor fișiere, directoare sau extensii de fișiere de la scanare.

Excepțiile vor fi folosite de către utilizatorii care au cunoștințe avansate privind computerele sau doar în situațiile următoare:

- Aveți un director mare pe sistemul dumneavoastră în care există filme și muzică
- Aveți o arhivă mare pe sistemul dumneavoastră în care păstrați diferite date.
- Păstrați un director în care să instalați diverse tipuri de software-uri și aplicații în scopuri de testare.Scanarea directorului poate duce la pierderea anumitor date.

Pentru a adăuga directorul pe lista de excepții, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Excluderi**.
5. Asigurați-vă că este activă opțiunea **Excepții fișiere** apăsând butonul corespunzător.
6. Faceți clic pe link-ul **Fișiere și directoare excluse**.

7. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
8. Faceți clic pe **Caută**, selectați directorul care doriți să fie exclus de la scanare și faceți clic pe **OK**.
9. Faceți clic pe **Adaugă** și apoi pe **OK** pentru a salva modificările și a închide fereastra.

12.5. Ce să fac atunci când Bitdefender a detectat un fișier curat ca fiind infectat?

Există situații când Bitdefender marchează în mod greșit un fișier legitim ca fiind o amenințare. Pentru a corecta această eroare, adăugați fișierul în secțiunea de excluderi a Bitdefender:

1. Dezactivați protecția antivirus în timp real a Bitdefender:
   a. Deschideți fereastra Bitdefender.
   b. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
   c. În fereastra **Prezentare setări**, selectați **Antivirus**.
   d. În fereastra **Setări antivirus**, selectați secțiunea **Shield**.
   e. Faceți clic pe comutator pentru a dezactiva **scanarea la accesare**.
2. Afișați elementele ascunse din Windows. Pentru a afla cum să procedați, consultați *„Cum pot afișa elementele ascunse din Windows?”* (p. 58).
3. Restaurați fișierul din zona de carantină:
   a. Deschideți fereastra Bitdefender.
   b. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
   c. În fereastra **Prezentare setări**, selectați **Antivirus**.
   d. În fereastra **Setări antivirus**, selectați secțiunea **Carantină**
   e. Selectați fișierul și faceți clic pe **Restabilire**.
4. Adăugați fișierul la lista de Excepții. Pentru a afla cum să procedați, consultați *„Cum exclud un director de la procesul de scanare?”* (p. 47).
5. Activați protecția antivirus în timp real a Bitdefender.
6. Contactați un reprezentant al echipei noastre de asistență tehnică și solicitați eliminarea semnăturii de detectare. Pentru a afla cum să procedați, consultați *„Solicitarea ajutorului”* (p. 156).

12.6. Cum aflu ce viruși au fost detectați de Bitdefender?

De fiecare dată când se efectuează o operațiune de scanare, se creează un jurnal în care Bitdefender înregistrează toate problemele detectate.

Raportul de scanare conține informații detaliate despre procesul de scanare înregistrat, cum ar fi opțiunile de scanare, locațiile scanate, amenințările găsite și acțiunile luate asupra acestor amenințări.

Puteți deschide raportul de scanare direct din programul asistent de scanare, după ce scanarea a luat sfârșit, apăsând **Afișează jurnal**.

Pentru a verifica un jurnal de scanare sau orice infestare detectată ulterior, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Evenimente** de pe bara de instrumente din partea superioară.
3. În fereastra **Prezentare evenimente**, selectați **Antivirus**.
4. În fereastra **Evenimente antivirus**, selectați secțiunea **Scanare viruși**. Aici puteți găsi toate evenimentele malware scanate, inclusiv amenințările detectate în urma scanării la accesare și a scanărilor inițiate la comanda utilizatorului și starea modificărilor pentru scanările automate.
5. În lista de evenimente puteți verifica ce operațiuni de scanare au fost realizate recent. Faceți clic pe un eveniment pentru a vizualiza detaliile acestuia.
6. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**. Jurnalul de scanare se va deschide într-o nouă fereastră.

13. Control Parental

13.1. Cum îmi protejez copiii împotriva amenințărilor online?

Opțiunea Control parental oferită de Bitdefender vă oferă posibilitatea de a restricționa accesul la internet și la anumite aplicații, astfel încât copiii dumneavoastră să nu poată vizualizeze site-uri și aplicații cu conținut neadecvat, atunci când nu vă aflați prin preajmă să-i supravegheați.

Pentru a configura Control parental, urmați pașii de mai jos:

1. Creați conturi de utilizator Windows limitate (standard) pentru copiii dumneavoastră. Pentru mai multe informații, consultați *„Cum creez conturi de utilizator Windows?"* (p. 52).
2. Asigurați-vă că sunteți conectat la calculator pe contul de administrator. Doar utilizatorii cu drepturi administrative pe sistem (administratorii de sistem) pot accesa și configura Controlul parental.
3. Configurați funcția de Control parental pentru conturile de utilizator folosite de copiii dumneavoastră.
   a. Deschideți fereastra Bitdefender.
   b. Faceți clic pe butonul **MyBitdefender** din partea de sus a ferestrei și selectați **Control Parental** din meniul derulant.
   c. Panoul de Control Parental se va deschide într-o nouă fereastră. De aici puteți verifica și configura setările funcției de Control Parental.
   d. Faceți clic pe **Adăugare copil** în meniul din stânga.
   e. Introduceți numele și vârsta copilului în secțiunea **Profil**. Setarea vârstei copilului va încărca automat setările considerate adecvate pentru respectiva categorie de vârstă, pe baza standardelor de dezvoltare a copilului.

Verificați activitatea copiiilor dumneavoastră și modificați setările de Control Parental folosind MyBitdefender de la orice calculator sau dispozitiv mobil conectat la Internet.

Pentru mai multe informații referitoare la utilizarea funcției de Control parental, consultați *„Control Parental "* (p. 118).

13.2. Cum pot restricționa accesul la Internet pentru copilul meu?

Odată ce ați configurat funcția de Control Parental, puteți bloca cu ușurință accesul la Internet pentru anumite perioade de timp.

Funcția de Control Parental Bitdefender vă permite să controlați accesul la Internet pentru copiii dumneavoastră chiar și atunci când nu sunteți acasă.

Pentru a restricționa accesul la Internet la anumite ore din zi, urmați pașii de mai jos:

1. Folosind orice dispozitiv cu acces la Internet, deschideți o fereastră de browser web.
2. Mergeți la:https://my.bitdefender.com
3. Conectați-vă la contul dumneavoastră cu ajutorul numelui de utilizator și parolei.
4. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
5. Selectați profilul copilului dumneavoastră din meniul din stânga.
6. Faceți clic  pe panoul **Web** pentru a accesa fereastra **Activitate web**.
7. Faceți clic pe **Programare**.
8. Selectați din grilă intervalele temporale în care accesul la internet este blocat.Puteți face clic pe celule individuale sau puteți face clic și trage pentru a acoperi perioade mai lungi de timp.Pentru a începe o selecție nouă, faceți clic pe **Resetare**.
9. Faceți clic pe **OK**.

Notă

Bitdefender va efectua actualizări în fiecare oră indiferent dacă accesul la internet este blocat.

13.3. Cum blochez accesul copilului meu la un anumit site web?

Funcția de Control Parental Bitdefender vă permite să controlați conținutul accesat de copilul dumneavoastră atunci când folosește calculatorul și să blocați accesul la un site web chiar și atunci când nu sunteți acasă.

Funcția de Control Parental Bitdefender vă permite să controlați accesul la Internet pentru copiii dumneavoastră chiar și atunci când nu sunteți acasă.

Pentru a bloca accesul la un site web, urmați pașii de mai jos:

1. Folosind orice dispozitiv cu acces la Internet, deschideți o fereastră de browser web.
2. Mergeți la:https://my.bitdefender.com
3. Conectați-vă la contul dumneavoastră cu ajutorul numelui de utilizator și parolei.
4. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
5. Selectați profilul copilului dumneavoastră din meniul din stânga.
6. Faceți clic  pe panoul **Web** pentru a accesa fereastra **Activitate web**.

7. Faceți clic pe **Listă restricții**.
8. Introduceți adresa de e-mail în câmpul corespunzător și faceți clic pe **Adăugare**.
9. Site-ul web a fost adăugat în lista de site-uri restricționate.

13.4. Cum împiedic copilul meu să se joace pe calculator?

Funcția de Control parental a Bitdefender vă permite să controlați conținutul pe care îl accesează copilul dumneavoastră în timp ce utilizează computerul.

Dacă doriți să restricționați accesul la un anumit joc sau o anumită aplicație, puteți folosi funcția de Control parental Bitdefender chiar și atunci când nu sunteți acasă.

Pentru a bloca accesul la un joc sau o aplicație, urmați pașii de mai jos:

1. Folosind orice dispozitiv cu acces la Internet, deschideți o fereastră de browser web.
2. Mergeți la:https://my.bitdefender.com
3. Conectați-vă la contul dumneavoastră cu ajutorul numelui de utilizator și parolei.
4. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
5. Selectați profilul copilului dumneavoastră din meniul din stânga.
6. Faceți clic  pe panoul **Aplicații** pentru a accesa fereastra **Activități aplicații**.
7. Faceți clic pe **Listă restricții**.
8. Introduceți (sau inserați prin copiere și lipire) în câmpul corespunzător calea către fișierul executabil.
9. Faceți clic pe **Adăugare** pentru a adăuga aplicația în **Lista de aplicații restricționate**.

13.5. Cum creez conturi de utilizator Windows?

Un cont de utilizator Windows reprezintă un profil unic care include toate setările, privilegiile și fișierele personale ale fiecărui utilizator în parte. Conturile Windows permit administratorului calculatorului să controleze accesul fiecărui utilizator.

Configurarea de conturi de utilizator este utilă atunci când calculatorul este utilizat în comun de părinți și copii - un părinte poate configura conturi pentru fiecare copil în parte.

Alegeți sistemul de operare pe care îl aveți pentru a afla cum puteți crea conturi Windows.

- Windows XP:
  1. Conectați-vă la calculatorul dumneavoastră pe un cont de administrator.
  2. Faceți clic pe Start, Panoul de comandă și apoi faceți clic pe Conturi de utilizator.

3. Faceți clic pe Creare cont nou.
4. Introduceți numele utilizatorului. Puteți utiliza numele întreg al persoanei, prenumele sau porecla acesteia. Apoi faceți clic pe Înainte.
5. La tipul de cont, selectați Limitat și apoi Creează cont. Conturile limitate sunt potrivite pentru copii deoarece aceștia nu pot realiza modificări la nivelul întregului sistem sau instala anumite aplicații.
6. Noul dumneavoastră cont va fi creat și îl veți vedea listat pe ecranul de Administrare a conturilor.

- Windows Vista sau Windows 7:

1. Conectați-vă la calculatorul dumneavoastră pe un cont de administrator.
2. Faceți clic pe Start, Panoul de comandă și apoi faceți clic pe Conturi de utilizator.
3. Faceți clic pe Creare cont nou.
4. Introduceți numele utilizatorului. Puteți utiliza numele întreg al persoanei, prenumele sau porecla acesteia. Apoi faceți clic pe Înainte.
5. Pentru tipul de cont, faceți clic pe Standard și apoi Creați cont. Conturile limitate sunt potrivite pentru copii deoarece aceștia nu pot realiza modificări la nivelul întregului sistem sau instala anumite aplicații.
6. Noul dumneavoastră cont va fi creat și îl veți vedea listat pe ecranul de Administrare a conturilor.

Notă

După ce ați adăugat noi conturi de utilizator, puteți crea parole pentru conturi.

14. Control date

14.1. Cum mă asigur că tranzacțiile mele online sunt securizate?

Pentru a asigura confidențialitatea operațiunilor pe care le efectuați online, puteți folosi browserul furnizat de Bitdefender, care vă protejează tranzacțiile și aplicațiile de home banking.

Bitdefender Safepay este un browser securizat creat special pentru a vă proteja datele cardului de credit, numărul de cont sau alte date confidențiale pe care le puteți introduce atunci când accesați diferite site-uri.

Pentru a vă menține activitatea online în deplină siguranță și confidențialitate, urmați pașii de mai jos:

1. Faceți dublu clic pe pictograma Bitdefender Safepay de pe desktop.

   Se va deschide browserul Bitdefender Safepay.

2. Faceți clic pe butonul  pentru a accesa **Tastatura virtuală**.
3. Folosiți **Tastatura virtuală** atunci când introduceți informații confidențiale, cum ar fi parolele.

14.2. Cum îmi protejez contul de Facebook?

Safego este o aplicație pentru Facebook dezvoltată de Bitdefender pentru a menține siguranța contului activat pe rețeaua de socializare.

Rolul său este de a scana link-urile pe care le primiți de la prietenii de pe Facebook și de a monitoriza setările de confidențialitate a contului dumneavoastră.

Pentru a accesa Safego din produsul Bitdefender, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Safego**, faceți clic pe **Administrare** și selectați **Activează pentru Facebook** din meniul derulant. Veți fi direcționat către contul dumneavoastră.

   Dacă ați activat deja Safego pentru Facebook, veți putea să accesați statisticile referitoare la activitatea sa făcând clic pe butonul **Vizualizare rapoarte pentru Facebook**.
3. Utilizați informațiile de autentificare Facebook pentru a vă conecta la aplicația Safego.
4. Permiteți opțiunii Safego să acceseze contul dumneavoastră de Facebook.

14.3. Cum șterg definitiv un fișier cu ajutorul Bitdefender?

Dacă doriți să ștergeți definitiv un fișier din sistemul dumneavoastră, este necesar să ștergeți fizic datele de pe hard disk.

Funcția Ștergere definitivă fișiere a Bitdefender vă permite să ștergeți definitiv și rapid fișiere și directoare din computerul dumneavoastră, cu ajutorul meniului contextual Windows, urmând pașii de mai jos:

1. Faceți clic dreapta pe fișierul sau directorul pe care doriți să-l ștergeți definitiv, alegeți Bitdefender și selectați **Ștergere definitivă fișiere**.
2. Va apărea o fereastră de configurare. Faceți clic pe **Da** pentru a porni asistentul Ștergere definitivă fișiere.
3. Așteptați ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.
4. Sunt afișate rezultatele. Faceți clic pe **Închide** pentru a părăsi asistentul.

15. Informații utile

15.1. Cum închid automat calculatorul după finalizarea operațiunii de scanare?

Bitdefender oferă mai multe opțiuni de scanare pe care le puteți folosi pentru a vă asigura că sistemul dumneavoastră nu este infectat cu programe periculoase. Scanarea întregului calculator poate dura destul de mult timp, în funcție de configurația hardware și software a sistemului dumneavoastră.

Din acest motiv, Bitdefender vă permite să configurați Bitdefender să închidă sistemul imediat după finalizarea scanării.

Spre exemplu: v-ați terminat lucrul la calculator și vreți să mergeți la culcare. Doriți să efectuați o verificare integrală a sistemului dumneavoastră în vederea detectării programelor periculoase cu ajutorulBitdefender.

Iată cum trebuie să configurați Bitdefender pentru a închide automat sistemul la finalizarea scanării:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antivirus**, faceți clic pe **Scanează acum** și selectați **Scanare personalizată** din meniul derulant.
3. Faceți clic pe **Adaugă obiect** pentru a selecta fișierele sau directoarele ce vor fi scanate.
4. Dacă doriți să configurați în detaliu opțiunile de scanare, faceți clic pe **Opțiuni scanare**.
5. Selectați opțiunea de închidere a calculatorului după finalizarea scanării în cazul în care nu a fost detectată nicio amenințare.
6. Faceți clic pe **Pornire scanare**.

Dacă nu este detectată nicio amenințare, calculatorul se va închide.

Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora. Pentru mai multe informații, consultați *„Programul asistent de scanare”* (p. 73).

15.2. Cum pot configura Bitdefender să utilizeze o conexiune la internet de tip proxy?

Dacă computerul dumneavoastră se conectează la internet prin intermediul unui server proxy, trebuie să configurați Bitdefender cu setările proxy. În mod normal, Bitdefender detectează și importă în mod automat setările proxy ale sistemului dumneavoastră.

Important
Conexiune de internet de acasă nu sunt folosite, în mod normal, ca server proxy. Ca regulă de bază, verificați și configurați setările conexiunii proxy ale programului Bitdefender atunci când nu funcționează actualizările. Dacă Bitdefender poate folosi actualizări, înseamnă că este configurat corespunzător pentru a se conecta la internet.

Pentru a gestiona setările proxy, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **General**.
4. În fereastra **Setări generale**, selectați secțiunea **Avansat**.
5. Activați consumul proxy făcând clic pe buton.
6. Faceți clic pe link-ul **Administrare proxy**.
7. Există două opțiuni de configurare a setărilor proxy:
   - **Importă setări proxy din browserul implicit** - setări proxy ale utilizatorului curent, extrase din browserul implicit. Dacă serverul proxy necesită un nume de utilizator și o parolă pentru autentificare, atunci va trebui să le specificați în câmpurile corespunzătoare.

     Notă
     Bitdefender poate importa setări proxy de la browserele cele mai des folosite, inclusiv cele mai noi versiuni pentru Internet Explorer, Mozilla Firefox și Opera.

   - **Setări proxy personalizate** - setări proxy pe care le puteți configura cum doriți. Următoarele setări trebuie specificate:
     - **Adresă** - introduceți adresa IP a serverului proxy.
     - **Port** - introduceți portul folosit Bitdefender pentru a se conecta la serverul proxy.
     - **Nume utilizator** - introduceți un nume de utilizator recunoscut de proxy.
     - **Parolă** - introduceți o parolă validă pentru numele de utilizator introdus.
8. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Bitdefender va folosi setările proxy disponibile până când va reuși să se conecteze la internet.

15.3. Utilizez o versiune Windows pe 32 biți sau pe 64 biți?

Pentru a identifica dacă utilizați un sistem de operare pe 32 sau 64 de biți, urmați acești pași:

- Pentru **Windows XP**:
  1. Faceți clic pe **Start**.

2. Mergeți la **My Computer** din meniul **Start**.
3. Faceți clic-dreapta pe **My Computer** și selectați **Properties**.
4. Dacă vedeți **x64 Edition** sub **System**, sistemul care rulează pe calculatorul dumneavoastră este o versiune Windows XP pe 64 biți.

   Dacă nu vedeți **x64 Edition** în listă, sistemul care rulează pe computerul dumneavoastră este o versiune Windows XP pe 32 biți.

- Pentru **Windows Vista** și **Windows 7**:

  1. Faceți clic pe **Start**.
  2. Localizați **Computer** din meniul **Start**.
  3. Faceți clic-dreapta pe **Computer** și selectați **Properties**.
  4. Sub **System** veți găsi informații referitoare la sistemul dumneavoastră.

15.4. Cum pot afișa elementele ascunse din Windows?

Acești pași sunt utili în acele cazuri în care aveți de-a face cu o situație în care este implicat un malware și trebuie să găsiți și să eliminați fișierele infectate, care pot fi ascunse.

Urmați acești pași pentru a afișa obiectele ascunse din Windows:

1. Faceți clic pe **Start**, mergeți la **Control Panel** și selectați **Folder Options**.
2. Mergeți la fila **View**.
3. Selectați **Display contents of system folders** (exclusiv pentru Windows XP).
4. Selectați **Show hidden files and folders**.
5. Debifați **Hide file extensions for known file types**.
6. Debifați **Hide protected operating system files**.
7. Faceți clic pe **Aplicare** și apoi pe **OK**.

15.5. Cum dezinstalez alte soluții de securitate?

Principalul motiv pentru utilizarea unei soluții de securitate este de a asigura protecția și siguranța datelor dumneavoastră. Ce se întâmplă însă când aveți mai multe produse de securitate instalate în același sistem?

Atunci când utilizați mai multe soluții de securitate pe același calculator, sistemul devine instabil. Programul de instalare a Bitdefender Internet Security 2013 detectează în mod automat alte programe de securitate și vă oferă opțiunea de a le dezinstala.

Dacă nu ați dezinstalat celelalte soluții de securitate în timpul instalării inițiale, urmați acești pași:

- Pentru **Windows XP**:
  1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Add / Remove programs**.
  2. Așteptați câteva momente până când este afișată lista programelor instalate.
  3. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Remove**.
  4. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
- Pentru **Windows Vista** și **Windows 7**:
  1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programs and Features**.
  2. Așteptați câteva momente până când este afișată lista programelor instalate.
  3. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Uninstall**.
  4. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

Dacă nu reușiți să dezinstalați cealaltă soluție de securitate, faceți rost de instrumentul de dezinstalare de pe site-ul web al furnizorului sau contactați-l direct pentru a vă oferi instrucțiuni de dezinstalare.

15.6. Cum folosesc funcția System Restore în Windows?

Dacă nu puteți porni computerul în modul normal, porniți-l în Safe Mode și, cu ajutorul System Restore, reveniți la un moment când puteați porni computerul fără probleme.

Pentru a putea efectua o restabilire a sistemului, trebuie să fiți autentificat pe Windows în calitate de administrator.

Pentru a folosi funcția System Restore, urmați pașii de mai jos:

- Pentru Windows XP:
  1. Conectați-vă la Windows în Safe Mode.
  2. Urmați această cale din meniul de start Windows: **Start → All Programs → System Tools → System Restore**.
  3. Pe pagina **Welcome to System Restore**, selectați prin clic opțiunea **Restore my computer to an earlier time** și apoi faceți clic pe Next.
  4. Pentru a porni sistemul în modul normal, urmați pașii programului asistent.
- Pentru Windows Vista și Windows 7:
  1. Conectați-vă la Windows în Safe Mode.
  2. Urmați această cale din meniul de start Windows: **All Programs → Accessories → System Tools → System Restore**.
  3. Pentru a porni sistemul în modul normal, urmați pașii programului asistent.

15.7. Cum pot să repornesc sistemul în Safe Mode?

Safe Mode este un mod de funcționare de diagnosticare, utilizat în principal pentru depanarea problemelor care afectează funcționarea normală a sistemului Windows. Printre astfel de probleme se numără driverele incompatibile și virușii ce împiedică pornirea normală a sistemului Windows. În Safe Mode funcționează numai câteva aplicații, iar Windows încarcă doar driverele de bază și un minim de componente ale sistemului de operare. Acesta este motivul pentru care majoritatea virușilor sunt inactivi atunci când Windows se află în Safe Mode și pot fi eliminați cu ușurință.

Pentru a porni Windows în Safe Mode:

1. Reporniți calculatorul.
2. Apăsați tasta **F8** de mai multe ori înainte ca Windows să pornească pentru a avea acces la meniul de pornire.
3. Selectați **Safe Mode** din meniul de pornire sau **Safe mode with Networking** dacă doriți să aveți acces la internet.
4. Apăsați **Enter** și așteptați până când Windows se încarcă în Safe Mode.
5. Acest proces se finalizează cu un mesaj de confirmare. Faceți clic pe **OK** pentru a confirma.
6. Pentru a porni Windows în mod normal, reporniți pur și simplu sistemul.

Administrarea securității dumneavoastră

16. Protecție antivirus

Bitdefender vă protejează calculatorul împotriva oricăror amenințări malware (viruși, troieni, aplicații spyware, rootkituri și altele).Protecția oferită de Bitdefender se împarte în două categorii:

- Scanarea la accesare - previne pătrunderea noilor amenințări malware în sistemul dumneavoastră.Bitdefender va scana, de exemplu, un document Word atunci când îl deschideți și un mesaj e-mail atunci când îl primiți.

  Procesul de scanare la accesare asigură protecție în timp real împotriva programelor malware, fiind o componentă esențială a oricărui program de securitate pentru calculatoare.

  Important
  Pentru a preveni infectarea computerului, păstrați activată funcția de **scanare la accesare**.

- Scanarea la cerere - permite detectarea și eliminarea virușilor și a altor coduri periculoase care există deja în sistemul dumneavoastră.Acesta este modul clasic de scanare, inițiată de utilizator – dumneavoastră alegeți partițiile, directoarele sau fișierele pe care trebuie să le scaneze Bitdefender, iar Bitdefender le scanează – la cerere.

  Atunci când este activată Scanarea automată, nu este necesar să activați manual scanările antimalware.Cu ajutorul opțiunii de Scanare automată, computerul dumneavoastră va fi scanat în mod repetat și vor fi aplicate acțiuni corespunzătoare în cazul în care sunt detectate acțiuni periculoase.Auto Scan rulează numai atunci când există suficiente resurse de sistem pentru a nu încetini funcționarea computerului.

Bitdefender scanează în mod automat orice fișier media amovibil care este conectat la computer pentru a vă asigura că este sigur să îl accesați.Pentru mai multe informații, consultați *„Scanarea automată a suporturilor media amovibile”* (p. 77).

Utilizatorii avansați pot configura excepțiile de la scanare în cazul în care nu doresc ca anumite fișiere sau tipuri de fișiere să fie scanate.Pentru mai multe informații, consultați *„Configurarea excepțiilor de la scanare”* (p. 78).

Atunci când detectează un virus sau un alt cod periculos, Bitdefender va încerca în mod automat să elimine codul periculos din fișierul infectat și să reconstruiască fișierul original.Această operațiune este denumită dezinfectare.Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere.Pentru mai multe informații, consultați *„Gestionarea fișierelor aflate în carantină”* (p. 81).

În cazul în care calculatorul dumneavoastră a fost infectat cu malware, consultați *„Eliminarea programelor malware din sistemul dumneavoastră”* (p. 146).Pentru a vă

ajuta să v ă curățați computerul de programele malware care nu pot fi eliminate din sistemul de operare Windows, Bitdefender vă pune la dispoziție Modul de salvare.Acesta este un mediu sigur, creat în special pentru eliminare acțiunilor malware, care vă permite să porniți computerul în mod independent de Windows.Atunci când computerul rulează în Modul de salvare, Windows malware este inactiv și, în consecință, poate fi șters cu ușurință.

Pentru a vă proteja împotriva aplicațiilor periculoase, Bitdefender folosește Active Virus Control, o tehnologie euristică avansată care monitorizează în permanență aplicațiile ce rulează pe sistemul dumneavoastră.Active Virus Control blochează în mod automat aplicațiile care prezintă un comportament tipic malware pentru a preveni daunele pe care le pot provoca acestea asupra computerului dumneavoastră.Ocazional, pot fi blocate aplicații legitime. În astfel de situații, puteți configura Active Virus Control să nu blocheze aceste aplicații a doua oară, creând reguli de excludere.Pentru a afla mai multe, consultați *„Active Virus Control”* (p. 82).

Multe forme de programe malware sunt create să infecteze sistemele, exploatându-le vulnerabilitățile, ca de exemplu actualizări de sistem care lipsesc sau aplicații neactualizate.Bitdefendervă ajută să identificați și să soluționați cu ușurință vulnerabilitățile sistemului pentru a asigura securitatea computerului dumneavoastră împotriva programelor malware și împotriva hacker-ilor.Pentru mai multe informații, consultați *„Remedierea vulnerabilităților sistemului”* (p. 84).

16.1. Scanare la accesare (protecție în timp real)

Bitdefender oferă protecție continuă în timp real împotriva unui număr mare de amenințări malware scanând toate fișierele accesate, mesajele e-mail și comunicațiile prin programe de mesagerie instant (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Setările implicite de protecție în timp real asigură o bună protecție împotriva malware cu un impact minor asupra performanțelor sistemului.Puteți modifica ușor setările de protecție în timp real în funcție de dorințele dumneavoastră prin comutarea la unul dintre nivelurile de protecție predefinite.Sau, dacă sunteți un utilizator experimentat, puteți configura setările de scanare în detaliu prin crearea unui nivel de protecție personalizat.

16.1.1. Activarea sau dezactivarea protecției în timp real

Pentru a activa sau dezactiva protecția în timp real împotriva programelor periculoase, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.

4. În fereastra **Setări antivirus**, selectați secțiunea **Shield**.
5. Faceți clic pe comutator pentru a activa sau dezactiva opțiunea de scanare la accesare.
6. Dacă doriți să dezactivați protecția în timp real, va apărea o fereastră de avertizare.Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării protecției în timp real. Puteți dezactiva protecția în timp real pentru 5, 15 sau 30 minute, pentru o oră, permanent sau doar până la repornirea sistemului.

Avertisment

Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați protecția în timp real pentru cât mai puțin timp posibil. Dacă protecția în timp real este dezactivată, nu veți mai fi protejat împotriva amenințărilor malițioase.

16.1.2. Reglarea nivelului de protecție în timp real

Nivelul de protecție în timp real definește setările de scanare pentru acest tip de protecție.Puteți modifica ușor setările de protecție în timp real în funcție de dorințele dumneavoastră prin comutarea la unul dintre nivelurile de protecție predefinite.

Pentru a ajusta nivelul de protecție în timp real, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Shield**.
5. Trageți de cursor de-a lungul scalei pentru a seta nivelul de protecție dorit.Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de protecție care se potrivește mai bine nevoilor dumneavoastră de securitate.

16.1.3. Configurarea setărilor de protecție în timp real

Utilizatorii avansați pot beneficia în urma ofertelor Bitdefender în ceea ce privește setările de scanare.Puteți configura setările protecției în timp real în detaliu prin crearea unui nivel de protecție personalizat.

Pentru a configura setările de protecție în timp real, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Shield**.
5. Faceți clic pe **Personalizare**.

6. Configurați setările de scanare după cum este nevoie.
7. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Informații cu privire la opțiunile de scanare

Aceste informații vă pot fi de folos:

- Dacă nu sunteți familiarizat cu anumiți termeni, verificați-i în glosar.De asemenea, puteți găsi informații utile pe Internet.
- **Opțiuni de scanare pentru fișierele accesate.** Puteți seta Bitdefender să scaneze toate fișierele sau doar aplicațiile scanate (fișiere de program).Scanarea tuturor fișierelor accesate asigură cea mai bună protecție, în timp ce scanarea exclusivă a aplicațiilor poate fi utilizată pentru asigurarea unei performanțe ridicate a sistemului.

  În mod implicit, atât directoarele locale, cât și partajările în rețea fac obiectul scanării la accesare.Pentru performanțe superioare ale sistemului, puteți exclude locațiile din rețea din scanarea la accesare.

  Aplicațiile (sau fișierele de program) sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere.Această categorie include următoarele extensii de fișiere:

  ```
  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt;
  accdu; acl; acr; action; ade; adp; air; app; as; asd; asp;
  awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl;
  csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm;
  dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv;
  hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar;
  js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr;
  mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg;
  msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg;
  ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx;
  ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg;
  pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox;
  rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm;
  snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe;
  vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf;
  xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx;
  xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
  ```

- **Scanează arhivele.** Scanarea în interiorul arhivelor este un proces lent și care necesită multe resurse, nefiind recomandată, prin urmare, pentru protecția în timp real.Arhivele ce conțin fișiere infectate nu reprezintă o amenințare imediată la adresa securității sistemului dumneavoastră.Codurile periculoase (malware) vă pot afecta sistemul numai dacă fișierul infectat este extras din arhivă și este executat fără a avea activată protecția în timp real.

Dacă decideți să utilizați această opțiune, puteți stabili o limită maximă acceptată de mărime pentru arhivele ce vor fi scanate la accesare.Selectați căsuța corespunzătoare și introduceți dimensiunea maximă a arhivei (exprimată în MB).

- **Opțiuni de scanare pentru traficul e-mail, web și de mesagerie instant.** Pentru a împiedica descărcarea fișierelor infectate pe calculatorul dumneavoastră, Bitdefender scanează automat următoarele puncte de intrare:
  - e-mail-uri primite sau trimise
  - trafic web
  - fișiere primite prin intermediul Yahoo! Messenger

  Scanarea traficului web poate încetini puțin navigarea pe internet, însă aceasta va bloca programele malware provenite de pe internet, inclusiv descărcările ascunse.

  Deși nu se recomandă, puteți dezactiva funcția de scanare antivirus a e-mailurilor, paginilor web sau a mesageriei instantant pentru a spori performanțele sistemului.Dacă dezactivați opțiunile de scanare corespunzătoare, e-mailurile și fișierele primite sau descărcate de pe internet nu vor fi scanate, permițând astfel fișierelor infectate să fie salvate pe calculatorul dumneavoastră.Aceasta nu reprezintă o amenințare majoră deoarece protecția în timp real va bloca programul malware atunci când fișierele infectate sunt accesate (deschise, mutate, copiate sau executate).

- **Scanează sectoarele de boot.** Puteți seta Bitdefender să scaneze sectoarele de boot ale hard-discului.Acest sector al hard disk-ului conține codul de computer necesar pentru a iniția procesul de boot.Atunci când un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.

- **Scanează numai fișierele noi și cele modificate .** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.

- **Scanare după keyloggers.** Selectați această opțiune pentru a scana sistemul în vederea identificării aplicațiilor de tip keylogger.Aplicațiile keyloggers înregistrează ceea ce introduceți de pe tastatură și trimit raporte pe Internet către o persoană rău intenționată (hacker).Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole și numere de conturi bancare, pe care le va folosi în beneficiul propriu.

Acțiuni luate împotriva atacurilor malware detectate

Puteți configura acțiunile inițiate de protecția în timp real.

Pentru a configura acțiunile, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.

3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Shield**.
5. Faceți clic pe **Personalizare**.
6. Configurați setările de scanare după cum este nevoie.
7. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Acțiunile de mai jos pot fi inițiate de protecția în timp real în Bitdefender:

Administrează acțiunile corespunzător

Bitdefender va aplica acțiunile recomandate în funcție de tipul fișierului detectat:

- **Fișiere infectate.** Fișierele detectate ca fiind infectate se potrivesc unei semnături malware din baza de date cu semnături malware a Bitdefender.Bitdefender va încerca în mod automat să elimine codul malware din fișierul infectat și să refacă fișierul original.Această operațiune este denumită dezinfectare.

  Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere.Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.Pentru mai multe informații, consultați *„Gestionarea fișierelor aflate în carantină”* (p. 81).

  Important

  Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este în întregime rău intenționat. În astfel de situații, fișierul infectat este șters de pe disk.

- **Fișiere suspecte.** Fișierele sunt identificate ca fiind suspecte în urma analizei euristice.Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare. Acestea vor fi mutate în carantină pentru a preveni o posibilă infectare.

  Implicit, fișierele aflate în carantină sunt trimise automat către Laboratoarele Bitdefender pentru a fi analizate de cercetătorii Bitdefender în materie de malware.Dacă este confirmată prezența unui program periculos, va fi lansată o semnătură care să permită ștergerea acestuia.

- **Arhive ce conțin fișiere infectate.**
  - Arhivele care conțin doar fișiere infectate sunt șterse în mod automat.
  - Dacă o arhivă conține atât fișiere infectate cât și fișiere curate, Bitdefender va încerca să șteargă fișierele infectate cu condiția să poată apoi reface arhiva cu fișierele curate.Dacă reconstrucția arhivei nu este posibilă, veți fi notificat de faptul că nu poate fi aplicată nicio acțiune astfel încât să se evite pierderea fișierelor curate.

Mută fișierele în carantină
Mută fișierele detectate în carantină.Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.Pentru mai multe informații, consultați *„Gestionarea fișierelor aflate în carantină”* (p. 81).

Interzice accesul
În caz că un fișier este infectat, accesul la acesta va fi interzis.

16.1.4. Restaurarea setărilor implicite

Setările implicite de protecție în timp real asigură o bună protecție împotriva malware cu un impact minor asupra performanțelor sistemului.

Pentru a restabili setările implicite pentru protecția în timp real, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. Faceți clic pe **Antivirus** în meniul din stânga și apoi pe fila **Scut**.
4. Faceți clic pe **Implicit**.

16.2. Scanare la cerere

Principalul obiectiv Bitdefender este protejarea calculatorului dumneavoastră de viruși. Aceasta se face în primul rând nepermițând virușilor noi să pătrundă în sistem, prin scanarea mesajelor e-mail și a fișierelor descărcate sau copiate pe calculator.

Există însă riscul ca un virus să fi fost în sistem înainte de instalarea Bitdefender. Din acest motiv, este indicat să vă scanați calculatorul de viruși după instalarea Bitdefender. Și este, de asemenea, recomandat să vă scanați sistemul periodic.

Scanarea la cerere se bazează pe sarcinile de scanare. Sarcinile de scanare sunt cele care specifică opțiunile de scanare și obiectele care să fie scanate.Puteți scana computerul oricând doriți prin executarea activităților implicite sau a propriilor activități (activități definite de utilizator).Dacă doriți să scanați anumite locații de pe computerul dumneavoastră sau să configurați opțiunile de scanare, puteți configura și rula o scanare personalizată.

16.2.1. Autoscanare

Scanarea automată reprezintă o scanare rapidă la cerere care scanează în mod discret toate datele dumneavoastră verificând să nu existe malware și aplică acțiunile corespunzătoare în cazul infectărilor detectate. Scanarea automată detectează și folosește intervale de timp pentru a efectua scanări repetate ale întregului sistem, atunci când consumul de resurse de sistem scade sub un anumit prag.

Beneficiile utilizării opțiunii de scanare automată:

- Impactul asupra sistemului este aproape zero.
- Prin prescanarea întregului hard disk, următoarele activități de scanare la cerere vor fi finalizate extrem de ușor.
- De asemenea, scanare la accesare va dura foarte puțin timp.

Pentru a activa sau dezactiva funcția de scanare automată, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antivirus**, faceți clic pe buton pentru a activa sau dezactiva **Scanarea automată**.

16.2.2. Scanarea unui fișier sau a unui director pentru detectarea malware

Trebuie să scanați fișierele și directoarele ori de câte ori considerați că acestea pot fi infectate.Faceți clic dreapta pe fișierul sau directorul pe care doriți să îl scanați, indicați **Bitdefender** și selectați **Scanează cu Bitdefender**.Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.După finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.

16.2.3. Rularea unei scanări rapide

Scanarea rapidă utilizează o tehnologie de scanare "in-the-cloud" (online) pentru a detecta aplicațiile periculoase ce rulează pe sistemul dumneavoastră. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o fracțiune din resursele de sistem necesare pentru o scanare antivirus obișnuită.

Pentru a executa o scanare rapidă, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antivirus**, faceți clic pe **Scanează acum** și selectați **Scanare rapidă** din meniul derulant.
3. Urmați programul asistent de scanare antivirus pentru a finaliza scanarea.Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate.Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

16.2.4. Executarea unei scanări a sistemului

Sarcina de Scanare a sistemului scanează întregul calculator pentru identificarea tuturor tipurilor de programe periculoase care îi amenință securitatea, cum ar fi virușii, aplicațiile spion, adware, rootkiturile și altele.În cazul în care ați dezactivat opțiunea de Scanare automată, vă recomandăm să rulați o Scanare completă a sistemului cel puțin o dată pe săptămână.

Notă
Deoarece opțiunea de **Scanare a sistemului** efectuează o scanare atentă a întregului sistem, aceasta poate dura un timp. În consecință, este recomandat să executați această activitate într-un moment când nu utilizați computerul.

Înainte de a executa o Scanare a sistemului, se recomandă următoarele:

- Asigurați-vă că Bitdefender este actualizat cu semnăturile malware. Scanarea calculatorului folosind semnături vechi poate împiedica Bitdefender să detecteze noi aplicații malițioase descoperite după ultima actualizare efectuată.Pentru mai multe informații, consultați *„Actualizarea permanentă a Bitdefender"* (p. 36).
- Închideți toate programele deschise.

Dacă doriți să scanați anumite locații de pe computer sau pentru a configura opțiunile de scanare, puteți configura și rula o sarcină de scanare personalizată.Pentru mai multe informații, consultați *„Configurarea unei scanări personalizate"* (p. 70).

Pentru a executa o Scanare a sistemului, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antivirus**, faceți clic pe **Scanează acum** și selectați **Scanare sistem** din meniul derulant.
3. Urmați programul asistent de scanare antivirus pentru a finaliza scanarea.Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor infectate.Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

16.2.5. Configurarea unei scanări personalizate

Pentru a configura o scanare antimalware în detaliu și pentru a o lansa, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antivirus**, faceți clic pe **Scanează acum** și selectați **Scanare personalizată** din meniul derulant.
3. Dacă doriți, puteți relua rapid rularea scanării personalizate anterioare, făcând clic pe înregistrarea corespunzătoare din **Scanări recente** sau din lista **Scanări favorite**.
4. Faceți clic pe **Adăugare țintă**, selectați căsuțele corespunzătoare locațiilor care doriți să fie scanate împotriva programelor periculoase și apoi faceți clic pe **OK**.
5. Faceți clic pe **Opțiuni de scanare** dacă doriți să configurați opțiunile de scanare.Va apărea o nouă fereastră.Urmați acești pași:
   a. Puteți configura ușor opțiunile de scanare reglând nivelul de scanare. Trageți cursorul deasupra scalei pentru a seta nivelul de scanare dorit.Utilizați

descrierea din partea dreaptă a scalei pentru a identifica nivelul de scanare care se potrivește mai bine nevoilor dumneavoastră.

Utilizatorii avansați pot beneficia în urma ofertelor Bitdefender în ceea ce privește setările de scanare.Pentru a configura în detaliu opțiunile de scanare, faceți clic pe **Personalizare**. La sfârșitul acestei secțiuni, veți găsi informații privitoare la acestea.

b. De asemenea, puteți configura aceste opțiuni generale:

- **Rulează sarcina cu prioritate scăzută .** Reduce prioritatea procesului de scanare. Veți permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va crește.
- **Minimizează Asistent de scanare în bara de sistem .** Minimizează fereastra de scanare în bara de sistem. Faceți dublu-clic pe simbolul Bitdefender pentru a o deschide.
- Specificați acțiunea care trebuie luată în cazul în care nu sunt identificate niciun fel de amenințări.

c. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

6. Faceți clic pe **Pornire scanare** și urmați instrucțiunile asistentului de scanare antivirus pentru a finaliza operația de scanare.Procesul de scanare poate dura ceva timp, în funcție de locațiile ce vor fi scanate.După finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.

Salvarea unei scanări personalizate la favorite

Atunci când configurați și lansați o scanare personalizată, aceasta este adăugată pe o listă limitată de scanări recente.Dacă planificați să reutilizați o scanare personalizată pe viitor, puteți alege să o salvați în lista de scanări favorite.

Pentru a salva o scanare personalizată rulată recent în lista de scanări favorite, urmați pașii de mai jos:

1. Deschideți fereastra de configurare a scanării personalizate.
   a. Deschideți fereastra Bitdefender.
   b. În panoul **Antivirus**, faceți clic pe **Scanează acum** și selectați **Scanare personalizată** din meniul derulant.
2. Localizați scanarea dorită din lista **Scanări recente**
3. Puneți cursorul mouse-ului pe numele scanării, apoi faceți clic pe pictograma pentru a adăuga scanarea la lista de scanări favorite.

Scanările salvate ca favorite sunt marcate cu ajutorul pictogramei .Dacă faceți clic pe această pictogramă, activitatea de scanare este eliminată din lista activităților de scanare favorite.

Informații cu privire la opțiunile de scanare

Aceste informații vă pot fi de folos:

- Dacă nu sunteți familiarizat cu anumiți termeni, verificați-i în glosar.De asemenea, puteți găsi informații utile pe Internet.
- **Scanează fișiere.** Puteți seta Bitdefender să scaneze toate tipurile de fișiere sau doar aplicațiile (fișiere de program) only.Scanarea tuturor fișierelor asigură cea mai bună protecție în timp ce scanarea aplicațiilor poate fi utilizată pentru efectuarea unei scanări mai rapide.

  Aplicațiile (sau fișierele de program) sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere.Această categorie include următoarele extensii de fișiere: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Opțiuni de scanare a arhivelor.** Arhivele ce conțin fișiere infectate nu reprezintă o amenințare imediată la adresa securității sistemului dumneavoastră.Codurile periculoase (malware) vă pot afecta sistemul numai dacă fișierul infectat este extras din arhivă și este executat fără a avea activată protecția în timp real.Cu toate acestea, se recomandă să utilizați această opțiune pentru a detecta și elimina orice amenințare potențială chiar dacă nu este o amenințare imediată.

  Notă
  Scanarea fișierelor arhivate crește timpul total necesar pentru scanare și necesită mai multe resurse de sistem.

- **Scanează sectoarele de boot.** Puteți seta Bitdefender să scaneze sectoarele de boot ale hard-discului.Acest sector al hard disk-ului conține codul de computer necesar pentru a iniția procesul de boot.Atunci când un virus infectează sectorul

de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.

- **Scanare memorie.** Selectați această opțiune pentru a scana programele ce rulează în memoria sistemului dumneavoastră.
- **Scanează registrii.** Selectați această opțiunea pentru a scana seriile de registri.Windows Registry este o bază de date care stochează setările de configurare și opțiunile pentru componentele sistemului de operare Windows, precum și pentru aplicațiile instalate.
- **Scanează fișiere cookie.** Selectați această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe computerul dumneavoastră.
- **Scanează numai fișierele noi și cele modificate .** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
- **Ignorare înregistratoare de taste comerciale.** Selectați această opțiune dacă aveți instalat și folosiți un software comercial de înregistrare taste pe computerul dumneavoastră.Înregistratoarele comerciale de taste sunt software-uri legitime de monitorizare a computerului, a căror funcție de bază este de a înregistra tot ce este tastat pe tastatură.
- **Scanează după rootkituri.** Selectați această opțiune pentru a lansa procesul de scanare pentru identificarea rootkit-urilor și a obiectelor ascunse, cu ajutorul acestui software.

16.2.6. Programul asistent de scanare

Ori de câte ori inițiați o scanare la cerere (de exemplu, faceți clic pe un director, evidențiați Bitdefender și selectați **Scanează cu Bitdefender**), se inițiază asistentul de Scanare antivirus Bitdefender.Urmați instrucțiunile asistentului pentru a finaliza procesul de scanare.

Notă

Dacă asistentul de scanare nu apare, este posibil ca scanarea să fie configurată să ruleze discret, în fundal.Căutați iconița de scanare în curs în bara de sistem.Puteți face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

Pasul 1 - Realizarea scanării

Bitdefender va începe scanarea obiectelor selectate.Puteți vedea informații în timp real cu privire la starea scanării precum și statistici (inclusiv timpul consumat, o estimare a timpului rămas și numărul de amenințări detectate). Pentru mai multe detalii, faceți clic pe link-ul **Afișează mai multe**

Așteptați ca Bitdefender să finalizeze scanarea.Procesul de scanare poate dura cateva minute, în funcție de complexitatea scanării.

Oprirea sau întreruperea temporară a scanării. Puteți opri scanarea oricând doriți făcând clic pe **Stop&Da**. Veți sări direct la ultimul pas al programului asistent.Pentru a opri temporar procesul de scanare, faceți clic pe **Întrerupe**. Va trebui să faceți clic pe **Reia** pentru a relua scanarea.

Arhive protejate prin parolă. Atunci când este identificată o arhivă protejată prin parolă, în funcție de setările de scanare, este posibil să fiți rugat să introduceți parola.Arhivele protejate prin parolă nu pot fi scanate decât dacă furnizați parola.Sunt disponibile următoarele opțiuni:

- **Parolă.** Dacă doriți ca Bitdefender să scaneze arhiva, selectați această opțiune și introduceți parola.Dacă nu cunoașteți parola, selectați una dintre celelalte opțiuni.
- **Nu cere parolă și nu scana obiectul.** Selectând această opțiune, arhiva nu fi scanată.
- **Nu scana niciun obiect protejat cu parola.** Selectați această opțiune dacă doriți să nu vi se mai solicite introducerea parolei pentru arhivele protejate prin parolă.Bitdefender nu le va putea scana, dar va păstra o înregistrare în raportul de scanare.

Alegeți opțiunea dorită și faceți clic pe **OK** pentru a continua scanarea.

Pasul 2 - Selectarea acțiunilor

După finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.

Notă

Atunci când executați o scanare rapidă sau o scanare completă a sistemului, Bitdefender va aplica în mod automat acțiunile recomandate asupra fișierelor în timpul scanării.Dacă rămân amenințări nesoluționate, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

Obiectele infectate sunt afișate în grupuri, în funcție de codul malware cu care sunt infectate.Faceți clic pe linkul corespunzător unei amenințări pentru a afla mai multe informații despre obiectele infectate.

Puteți alege o acțiune globală care să fie luată asupra tuturor problemelor sau puteți alege acțiuni separate pentru fiecare grup de probleme.Una sau mai multe dintre opțiunile următoare pot apărea în meniu:

Administrează acțiunile corespunzător
Bitdefender va aplica acțiunile recomandate în funcție de tipul fișierului detectat:

- **Fișiere infectate.** Fișierele detectate ca fiind infectate se potrivesc unei semnături malware din baza de date cu semnături malware a Bitdefender.Bitdefender va încerca în mod automat să elimine codul malware din fișierul infectat și să refacă fișierul original.Această operațiune este denumită dezinfectare.

  Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere.Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.Pentru mai multe informații, consultați *„Gestionarea fișierelor aflate în carantină”* (p. 81).

  Important

  Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este în întregime rău intenționat. În astfel de situații, fișierul infectat este șters de pe disk.

- **Fișiere suspecte.** Fișierele sunt identificate ca fiind suspecte în urma analizei euristice.Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare. Acestea vor fi mutate în carantină pentru a preveni o posibilă infectare.

  Implicit, fișierele aflate în carantină sunt trimise automat către Laboratoarele Bitdefender pentru a fi analizate de cercetătorii Bitdefender în materie de malware.Dacă este confirmată prezența unui program periculos, va fi lansată o semnătură care să permită ștergerea acestuia.

- **Arhive ce conțin fișiere infectate.**
  - Arhivele care conțin doar fișiere infectate sunt șterse în mod automat.
  - Dacă o arhivă conține atât fișiere infectate cât și fișiere curate, Bitdefender va încerca să șteargă fișierele infectate cu condiția să poată apoi reface arhiva cu fișierele curate.Dacă reconstrucția arhivei nu este posibilă, veți fi notificat de faptul că nu poate fi aplicată nicio acțiune astfel încât să se evite pierderea fișierelor curate.

Șterge

Îndepărtează fișierele identificate de pe disc.

Dacă într-o arhivă sunt stocate fișiere infectate împreună cu fișiere curate, Bitdefender ca încerca să șteargă fișierele infectate și să refacă arhiva incluzând doar fișierele curate.Dacă reconstrucția arhivei nu este posibilă, veți fi notificat de faptul că nu poate fi aplicată nicio acțiune astfel încât să se evite pierderea fișierelor curate.

Nu lua nicio acțiune

Nu se va lua nicio acțiune asupra fișierelor detectate.După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.

Faceți clic pe **Continuă** pentru a aplica acțiunile specificate.

Pasul 3 - Rezumat

Atunci când Bitdefender a remediat toate problemele apărute, rezultatele scanării vor fi afișate într-o nouă fereastră.Dacă doriți informații complete cu privire la procesul de scanare, faceți clic pe **Afișează jurnal** pentru a vizualiza jurnalul de scanare.

Faceți clic pe **Închide** pentru a închide fereastra.

Important

În majoritatea cazurilor, Bitdefender va dezinfecta fișierele infectate detectate sau le va izola.Cu toate acestea, există anumite probleme care nu pot fi rezolvate automat.Dacă este necesar, reporniți sistemul pentru a finaliza procesul de curățare.Pentru mai multe informații și instrucțiuni privind modul de eliminare a programelor malware în mod manual, consultați *„Eliminarea programelor malware din sistemul dumneavoastră”* (p. 146).

16.2.7. Examinarea jurnalelor de scanare

De fiecare dată când efectuați o scanare, se creează un jurnal de scanare și evidențele Bitdefender detectate în fereastra Prezentare Antivirus.Raportul de scanare conține informații detaliate despre procesul de scanare înregistrat, cum ar fi opțiunile de scanare, locațiile scanate, amenințările găsite și acțiunile luate asupra acestor amenințări.

Puteți deschide raportul de scanare direct din programul asistent de scanare, după ce scanarea a luat sfârșit, apăsând **Afișează jurnal**.

Pentru a verifica un jurnal de scanare sau orice infestare detectată ulterior, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Evenimente** de pe bara de instrumente din partea superioară.
3. În fereastra **Prezentare evenimente**, selectați **Antivirus**.
4. În fereastra **Evenimente antivirus**, selectați secțiunea **Scanare viruși**. Aici puteți găsi toate evenimentele malware scanate, inclusiv amenințările detectate în urma scanării la accesare și a scanărilor inițiate la comanda utilizatorului și starea modificărilor pentru scanările automate.
5. În lista de evenimente puteți verifica ce operațiuni de scanare au fost realizate recent.Faceți clic pe un eveniment pentru a vizualiza detaliile acestuia.
6. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**.Raportul de scanare va fi deschis în browserul dumneavoastră implicit.

16.3. Scanarea automată a suporturilor media amovibile

Bitdefender detectează automat unitățile mobile de stocare pe care le conectați la computer și le scanează în fundal.Acest lucru este recomandat pentru a preveni pătrunderea virușilor și a altor aplicații periculoase pe calculatorul dumneavoastră.

Unitățile detectate fac parte din următoarele categorii:

- CD/DVD
- unități de stocare pe USB, cum ar fi memoriile flash sau hard discurile externe
- unități de rețea mapate (la distanță)

Puteți configura scanarea automată separat pentru fiecare categorie de dispozitive de stocare.Scanarea automată a partițiilor rețelei mapate este dezactivată implicit.

16.3.1. Cum funcționează?

Când detectează un dispozitiv de stocare amovibil, Bitdefender inițiază scanarea în fundal pentru depistarea programelor periculoase (cu condiția ca scanarea automată să fie activată pentru acel tip de dispozitiv).O pictogramă de scanare Bitdefender va fi afișată în bara de sistem.Puteți face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

Dacă opțiunea Pilot automat este activată, nu veți fi întrerupt de scanare.Scanarea va fi doar înregistrată, iar informații privind scanarea pot fi vizualizate în fereastra Evenimente

Dacă opțiunea Pilot automat este dezactivată:

1. Veți fi notificat prin intermediul unei ferestre pop-up că a fost detectat un nou dispozitiv și că aceasta este scanat.
2. În majoritatea cazurilor, Bitdefender elimină automat programele periculoase detectate sau izolează fișierele infectate în carantină.Dacă există amenințări nesoluționate după finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul acestora.

   Notă
   Luați în considerare faptul că nu se poate întreprinde nicio acțiune împotriva fișierelor suspecte detectate pe CD-uri/DVD-uri. De asemenea, nu se poate întreprinde nicio acțiune împotriva fișierelor infectate sau suspecte detectate pe unități mapate de rețea în absența privilegiilor respective.

3. În momentul în care scanarea este finalizată, va apărea fereastra cu rezultatele scanării care vă va informa dacă puteți accesa în siguranță fișierele regăsite pe suportul media amovibil.

Următoarele informații vă pot fi de folos:

- Vă rugăm să acordați atenție maximă atunci când folosiți un CD/DVD infectat cu programe malware, deoarece un program malware nu poate fi șters de pe CD/DVD (suportul media este de tip read-only). Asigurați-vă că protecția în timp real este activată pentru a preveni răspândirea acțiunilor periculoase în cadrul sistemuluiCea mai bună metodă este să copiați datele inmportante de pe CD pe sistemul dumneavoastră și apoi să aruncați CD-ul.
- Există posibilitatea ca, în unele cazuri, Bitdefender să nu poată elimina elementele periculoase din anumite fișiere din cauza unor constrângeri tehnice sau legale. Un astfel de exemplu este reprezentat de fișierele arhivate cu ajutorul unei tehnologii brevetate (acest lucru se întâmplă din cauză că arhiva nu poate fi recreată corect).

  Pentru a afla cum să procedați în cazul programelor periculoase, consultați *„Eliminarea programelor malware din sistemul dumneavoastră”* (p. 146).

16.3.2. Administrarea scanării a fișierelor media amovibile

Pentru a gestiona suporturile media amovibile, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Excluderi**.

Pentru cea mai bună protecție, este recomandat să activați funcția de scanare automată pentru toate tipurile de dispozitive de stocare amovibile.

Opțiunile de scanare sunt pre-configurate pentru a obține rata maximă de detecție.În cazul în care sunt detectate fișiere infectate, Bitdefender va încerca să le dezinfecteze (să elimine codul periculos) sau să le mute în carantină. Dacă ambele acțiuni eșuează, asistentul de scanare Antivirus vă va permite să specificați alte acțiuni pentru a fi aplicate în cazul fișierelor infectate.Opțiunile de scanare sunt standard și nu le puteți modifica.

16.4. Configurarea excepțiilor de la scanare

Bitdefender permite excluderea anumitor fișiere, directoare sau extensii de fișiere de la scanare. Această caracteristică are scopul de a evita interferențele cu munca dumneavoastră și poate ajuta la îmbunătățirea performanței sistemului.Excepțiile vor fi folosite de către utilizatorii care au cunoștințe avansate în ceea ce privește computerele. În caz contrar, pot fi folosite urmând recomandările unui reprezentant Bitdefender.

Puteți configura ca excepțiile să se aplice doar în cazul scanării la accesare sau scanării la cerere, sau în cazul ambelor scanări.Obiectele excluse de la scanarea la

acces nu vor fi scanate, indiferent dacă acestea sunt accesate de către dumneavoastră sau de către o aplicație.

Notă

Excepțiile NU se vor aplica în cazul scanării contextuale.Scanarea contextuală este o metodă de scanare la cerere: faceți clic-dreapta pe fișierul sau directorul pe care doriți să-l scanați și selectați **Scanează cu Bitdefender** .

16.4.1. Excluderea fișierelor sau directoarelor de la scanare

Pentru a exclude anumite fișiere sau directoare de la scanare, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Excluderi**.
5. Pentru a activa excepțiile pentru fișiere, utilizați comutatorul corespunzător.
6. Faceți clic pe link-ul **Fișiere și directoare excluse**.În fereastra care va apărea, puteți administra fișierele și directoarele excluse de la scanare.
7. Pentru a adăuga excepții, urmați pașii de mai jos:
   a. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
   b. Faceți clic pe **Caută**, selectați fișierul sau directorul care doriți să fie exclus de la scanare și faceți clic pe **OK**.Ca o alternativă, puteți introduce (sau copia și lipi) calea către fișier sau director în câmpul editabil.
   c. În mod implicit, fișierul sau directorul selectat este exclus atât de la scanarea la accesare cât și de la scanarea la cerere. Pentru a modifica când anume se aplică aceste excepții, selectați una dintre celelalte opțiuni.
   d. Faceți clic pe **Adaugă**.
8. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

16.4.2. Excluderea extensiilor de fișiere de la scanare

În momentul în care o extensie de fișier este exclusă de la scanare, Bitdefender nu va mai scana fișierele cu acea extensie, indiferent de locația acestora pe computer.Excepțiile pot fi aplicate, de asemenea, pentru fișierele aflate pe suporturi amovibile cum ar fi CD-urile, DVD-urile, dispozitivele USB sau unitățile de rețea.

Important

Acționați cu grijă atunci când excludeți extensii de la scanare deoarece asemenea excepții pot face computerul vulnerabil în fața acțiunilor periculoase.

Pentru a exclude de la scanare extensii de fișiere, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Excluderi**.
5. Pentru a activa excepțiile pentru fișiere, utilizați comutatorul corespunzător.
6. Faceți clic pe link-ul **Extensii excluse**În fereastra care va apărea, puteți administra extensiile de fișiere excluse de la scanare.
7. Pentru a adăuga excepții, urmați pașii de mai jos:
   a. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
   b. Introduceți extensiile ce doriți să fie excluse de la scanare, separându-le prin punct și virgulă (;).Iată un exemplu:

      ```
      txt;avi;jpg
      ```

   c. În mod implicit, toate fișierele care au extensiile specificate sunt excluse atât de la scanarea la accesare cât și de la scanarea la cerere. Pentru a modifica când anume se aplică aceste excepții, selectați una dintre celelalte opțiuni.
   d. Faceți clic pe **Adaugă**.
8. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

16.4.3. Administrarea excepțiilor de la scanare

Dacă excluderile de la scanare configurate nu mai sunt necesare, se recomandă să le ștergeți sau să dezactivați utilizarea lor.

Pentru a gestiona excepțiile de la scanare, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Excluderi**. Folosiți opțiunile din secțiune **Fișiere și directoare** pentru a gestiona excepțiile de la scanare.
5. Pentru a șterge sau a edita excepțiile de la scanare, faceți clic pe unul dintre link-urile disponibile.Procedați astfel:
   - Pentru a șterge o intrare din tabel, selectați-o și faceți clic pe butonul **Șterge**.
   - Pentru a edita o intrare din table, faceți dublu clic pe aceasta (sau selectați-o și faceți clic pe butonul **Editare**).Va apărea o nouă fereastră unde puteți schimba extensia sau calea care va fi exclusă, precum și tipul de scanare de

la care acestea să fie excluse. Efectuați modificările necesare, apoi faceți clic pe **Modifică**.

6. Pentru a dezactiva excepțiile de la scanare, utilizați comutatorul corespunzător.

16.5. Gestionarea fișierelor aflate în carantină

Bitdefender izolează fișierele infectate cu malware ce nu pot fi dezinfectate, precum și fișierele suspecte într-o zonă sigură numită carantină.Atunci când sunt în carantină virușii sunt inofensivi, pentru că nu pot fi executați sau citiți.

Implicit, fișierele aflate în carantină sunt trimise automat către Laboratoarele Bitdefender pentru a fi analizate de cercetătorii Bitdefender în materie de malware.Dacă este confirmată prezența unui program periculos, va fi lansată o semnătură care să permită ștergerea acestuia.

În plus, Bitdefender scanează fișierele din carantină după fiecare actualizare a semnăturilor malware.Fișierele curățate sunt mutate automat în locația lor originală.

Pentru a verifica și administra fișierele aflate în carantină, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Carantină**
5. Fișierele aflate în carantină sunt gestionat în mod automat de Bitdefender, în funcție de setările implicite pentru carantină.Deși nu este recomandat, puteți ajusta setările carantinei în funcție de preferințele dumneavoastră.

   Rescanează carantina după actualizarea definițiilor de viruși
   Mențineți activată această opțiune pentru a scana în mod automat fișiere aflate în carantină după fiecare actualizare a definițiilor de viruși.Fișierele curățate sunt mutate automat în locația lor originală.

   Trimiteți fișierele suspecte din carantină pentru o analiză ulterioară
   Mențineți această opțiune activată pentru ca fișierele aflate în carantină să fie trimise automat către Laboratoarele Bitdefender.Fișierele mostră vor fi analizate de către cercetătorii Bitdefender în materie de malware.Dacă este confirmată prezența unui program periculos, va fi lansată o semnătură care să permită ștergerea acestuia.

   Ștergere conținut mai vechi de {30} zile
   Implicit, fișierele aflate în carantină de mai mult de 30 de zile sunt șterse automat.Dacă doriți să schimbați acest interval, introduceți o nouă valoare în câmpul corespunzător.Pentru a dezactiva ștergerea fișierelor vechi aflate în paranteză, introduceți 0.

6. Pentru a șterge un fișier aflat în carantină, selectați-l și faceți clic pe butonul **Șterge**.Dacă doriți să restaurați un fișier aflat în carantină în locația sa originală, selectați-l și faceți clic pe **Restaurează**.

16.6. Active Virus Control

Bitdefender Active Virus Control este o tehnologie inovatoare de detecție proactivă, care folosește metode euristice avansate pentru a detecta potențiale amenințări în timp real.

Modulul Active Virus Control monitorizează continuu aplicațiile care rulează pe calculatorul dumneavoastră, căutând acțiuni periculoase. Fiecare dintre aceste acțiuni are un anumit punctaj iar punctajul global este calculat pentru fiecare proces.În cazul în care scorul total pentru un proces atinge un anumit prag, procesul este considerat dăunător și este blocat în mod automat.

Dacă funcția de Pilot automat este dezactivată, veți fi notificat prin intermediul unei ferestre pop-up despre aplicația blocată.În caz contrar, aplicația va fi blocată fără nicio notificare în prealabil.Puteți verifica ce aplicații au fost detectate de Active Virus Control, în fereastra Evenimente.

16.6.1. Verificarea aplicațiilor detectate

Pentru a verifica aplicațiile detectate de Active Virus Control, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Evenimente** de pe bara de instrumente din partea superioară.
3. În fereastra **Prezentare evenimente**, selectați **Antivirus**.
4. În fereastra **Evenimente antivirus**, selectați secțiunea **Control virus activ**
5. Faceți clic pe un eveniment pentru a vizualiza detaliile acestuia.
6. Dacă considerați că aplicația este sigură, puteți configura ca Active Virus Control să nu o mai blocheze pe viitor, făcând clic pe **Permite și monitorizează**.Active Virus Control va monitoriza în continuare aplicațiile excluse. Dacă sunt detectate acțiuni suspecte efectuate de o aplicație exclusă, acest eveniment va fi înregistrat și raportat către Bitdefender Cloud ca eroare de detecție.

16.6.2. Activarea sau dezactivarea funcției Active Virus Control

Pentru a activa sau dezactiva funcția Active Virus Control, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.

4. În fereastra **Setări antivirus**, selectați secțiunea **Shield**.
5. Faceți clic pe comutator pentru a activa sau dezactiva opțiunea Active Virus Control.

16.6.3. Ajustarea protecției Active Virus Control

În cazul în care Active Virus Control detectează adesea aplicații legitime, încercați să setați un nivel de protecție mai permisiv.

Pentru a ajusta protecția Active Virus Control, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Shield**.
5. Asigurați-vă că opțiunea Active Virus Control este activată.
6. Trageți de cursor de-a lungul scalei pentru a seta nivelul de protecție dorit.Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de protecție care se potrivește mai bine nevoilor dumneavoastră de securitate.

Notă
După ce setați un nivel de protecție superior, Active Virus Control va necesita mai puține semne de comportament tipic malware pentru a raporta un anumit proces. Acest lucru va contribui la raportarea unui număr mai mare de aplicații și, în același timp, la o probabilitate sporită de false pozitive (aplicații legitime detectate ca fiind nocive).

16.6.4. Administrarea proceselor excluse

Puteți configura regulile de excludere pentru aplicațiile sigure astfel încât Active Virus Control să nu blocheze aceste aplicații în cazul în care acestea întreprind acțiuni ce pot părea periculoase.Active Virus Control va monitoriza în continuare aplicațiile excluse. Dacă sunt detectate acțiuni suspecte efectuate de o aplicație exclusă, acest eveniment va fi înregistrat și raportat către Bitdefender Cloud ca eroare de detecție.

Pentru a gestiona excepțiile de la procesul Active Virus Control, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Excluderi**.

5. Faceți clic pe link-ul **Procese excluse**.În fereastra care va apărea, puteți gestiona excepțiile de la procesul Active Virus Control.

Notă
Excepțiile de proces se aplică de asemenea în cazul Sistemului de detecție a intruziunilor inclus în firewallul Bitdefender.

6. Pentru a adăuga excepții, urmați pașii de mai jos:
   a. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
   b. Faceți clic pe **Caută**, identificați și selectați aplicația care doriți să fie exclusă și faceți clic pe **OK**.
   c. Mențineți selectată opțiunea **Permite** pentru a preveni blocarea aplicației de către Active Virus Control.
   d. Faceți clic pe **Adaugă**.
7. Pentru a șterge sau pentru a edita excepțiile, urmați pașii de mai jos:
   - Pentru a șterge un obiect din listă, selectați-l și faceți clic pe butonul **Șterge**.
   - Pentru a edita o intrare din tabel, faceți dublu clic pe aceasta (sau selectați-o) și faceți clic pe butonul **Modificare**.Efectuați modificările necesare, apoi faceți clic pe **Modifică**.
8. Salvați schimbarea și închideți fereastra.

16.7. Remedierea vulnerabilităților sistemului

Un pas important în protejarea calculatorului dumneavoastră împotriva persoanelor răuvoitoare și a aplicațiilor periculoase este de a menține actualizat sistemul de operare și aplicațiile pe care le utilizați în mod regulat.Ar trebui, de asemenea, să luați în considerare dezactivarea setărilor Windows, care fac sistemul mai vulnerabil în fața programelor periculoase.De asemenea, pentru a preveni accesul fizic neautorizat la calculatorul dumneavoastră, trebuie configurate parole puternice (parole care nu pot fi ghicite cu ușurință) pentru fiecare cont de utilizator Windows.

Bitdefender permite remedierea cu ușurință a vulnerabilităților sistemului dumneavoastră prin oricare dintre cele două metode de mai jos:

- Puteți scana și remedia vulnerabilitățile sistemului, pas cu pas, cu ajutorul asistentului **Scanare vulnerabilități**.
- Prin intermediul monitorizării automate a vulnerabilităților, puteți verifica și remedia vulnerabilitățile detectate, în fereastra Evenimente.

Ar trebui să verificați și să remediați vulnerabilitățile sistemului săptămânal sau o dată la două săptămâni.

16.7.1. Scanarea sistemului pentru identificarea vulnerabilităților

Pentru a remedia vulnerabilitățile sistemului cu ajutorul asistentului de Scanare vulnerabilități, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antivirus**, faceți clic pe **Scanează acum** și selectați **Scanare vulnerabilitate** din meniul derulant.
3. Urmați procedura ghidată în șase pași pentru a îndepărta vulnerabilitățile din sistem.Puteți naviga prin programul asistent cu ajutorul butonului **Înainte**. Pentru a părăsi asistentul, faceți clic pe **Anulează**.

   a. **Protejați-vă calculatorul**

      Selectați vulnerabilitățile de verificat

   b. **Verificare probleme**

      Așteptați ca Bitdefender să finalizeze verificarea sistemului dumneavoastră în sensul descoperirii vulnerabilităților.

   c. **Actualizări Windows**

      Puteți vedea lista actualizărilor critice și normale pentru Windows care nu sunt instalate pe calculatorul dumneavoastră.Selectați actualizările pe care doriți să le instalați.

      Pentru a inițiia instalarea actualizărilor selectate, faceți clic pe **Înainte**.Rețineți că este posibil ca instalarea actualizărilor să dureze ceva timp iar pentru unele dintre ele poate fi necesară repornirea sistemului pentru ca instalarea să se finalizeze.Dacă este necesar, reporniți sistemul cât mai curând posibil.

   d. **Actualizări aplicații**

      Dacă o aplicație nu este la zi, faceți clic pe linkul furnizat pentru a descărca ultima versiune a acesteia.

   e. **Parole vulnerabile**

      Puteti vedea lista conturilor de utilizator Windows configurate pe calculatorul dumneavoastră și nivelul de protecție asigurat de parola acestora.

      Faceți clic pe **Remediază** pentru a modifica parolele simple.Puteți să-i solicitați utilizatorului să schimbe parola la următoarea autentificare sau puteți schimba dumneavoastră parola imediat.Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

   f. **Rezumat**

      Aici puteți vedea rezultatul operației.

16.7.2. Cu ajutorul monitorizării automate a vulnerabilităților

Bitdefender scanează sistemul împotriva vulnerabilităților la intervale regulate, în fundal și păstrează înregistrări ale problemelor detectate în fereastra Evenimente.

Pentru a verifica și remedia problemele detectate, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Evenimente** de pe bara de instrumente din partea superioară.
3. În fereastra **Prezentare evenimente**, selectați **Antivirus**.
4. În fereastra **Evenimente antivirus**, selectați secțiunea **Vulnerabilitate**.
5. Puteți vizualiza informații detaliate cu privire la vulnerabilitățile sistemului detectate.În funcție de problemă, pentru a remedia o anumită vulnerabilitate, procedați după cum urmează:
   - În cazul în care sunt disponibile actualizări Windows, faceți clic pe **Actualizează acum** pentru a deschide asistentul de scanare a vulnerabilităților apoi instalați actualizările.
   - Dacă o aplicație nu este actualizată, faceți clic pe **Actualizează acum** pentru a găsi un link către pagina furnizorului, de unde puteți instala cea mai recentă versiune a aplicației respective.
   - Dacă un cont de utilizator Windows are o parolă slabă, faceți clic pe **Repară parolă** pentru a forța utilizatorul să modifice parola la următoarea conectare sau schimbați-o chiar dumneavoastră.Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).
   - Dacă funcția de executare automată Windows este activată, faceți clic pe **Dezactivare** pentru a o dezactiva.

Pentru a configura setările de monitorizare a vulnerabilităților, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Evenimente antivirus**, selectați secțiunea **Vulnerabilitate**.
5. Faceți clic pe comutator pentru a activa sau dezactiva opțiunea de scanare automată a vulnerabilităților.

Important

Pentru a fi informat automat despre vulnerabilitățile sistemului sau aplicațiilor, mențineți funcția **Scanare automată a vulnerabilităților** activată.

6. Selectați vulnerabilitățile sistemului care doriți să fie verificate în mod regulat, cu ajutorul comutatoarelor corespunzătoare.

   Actualizări Windows importante

   Verificați dacă sistemul de operare Windows are instalate cele mai recente actualizări de securitate importante de la Microsoft.

   Actualizări Windows regulate

   Verificați dacă sistemul de operare Windows are instalate cele mai recente actualizări de securitate obișnuite de la Microsoft.

   Actualizări aplicații

   Verificați dacă aplicațiile importante ce folosesc internetul, instalate pe sistemul dumneavoastră sunt actualizate.Aplicațiile neactualizate pot fi exploatate de software-uri periculoase, expunându-vă computerul la atacuri din exterior.

   Parole vulnerabile

   Verificați dacă parolele pentru conturile de Windows configurate pe sistem sunt ușor de descoperit sau nu.Setând parole care sunt greu de ghicit (parole puternice), va fi mai mult mai dificil pentru hackeri să pătrundă în sistemul dumneavoastră.Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

   Executare automată a fișierelor media

   Verificați starea caracteristicii de executare automată Windows.Această caracteristică permite pornirea aplicațiilor în mod automat direct de pe CD, DVD, unități USB sau alte dispozitive externe.

   Anumite tipuri programe periculoase folosesc funcția de executare automată pentru a se răspândi de la suporturile media amovibile în computer. De aceea se recomandă să dezactivați această caracteristică Windows.

Notă

Dacă dezactivați monitorizarea pentru o anumită vulnerabilitate, posibilele probleme aferente nu vor mai fi înregistrate în fereastra Evenimente.

17. Antispam

Spam este un termen utilizat pentru a descrie un e-mail nesolicitat.Spamul este o problemă în creștere, atât pentru individ cât și pentru organizații. Nu este interesant, nu ați dori să fie văzut de către copii, puteți fi concediat din cauza lui (pentru pierdere de timp prin primirea de mesaje cu conținut sexual pe adresa de serviciu) și nu puteți împiedica trimiterea sa. Cel mai bun lucru pe care îl puteți face este, evident, să nu îl mai primiți. Din păcate, acesta există în cantități mari, într-o gamă largă de forme și mărimi.

Bitdefender Antispam utlizează remarcabile inovații tehnologice și filtre antispam standard pentru a ține la distanță spamul de căsuțele de mesaje ale utilizatorilor.Pentru mai multe informații, consultați *„Detalii privind modulul Antispam”* (p. 88).

Protecția antispam Bitdefender este disponibilă numai pentru clienții de e-mail configurați să primească mesaje e-mail prin protocolul POP3.POP3 este unul dintre cele mai des folosite protocoale de descărcare a mesajelor e-mail de pe un server de mail.

Notă

Bitdefender nu asigură protecție antispam pentru conturile de e-mail pe care le accesați prin intermediul serviciilor de e-mail oferite pe internet.

Mesajele spam detectate de Bitdefender sunt marcate cu prefixul `[spam]` în subiect.Bitdefender mută în mod automat mesajele spam într-un anumit director, după cum urmează:

- În Microsoft Outlook, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Deleted Items**.Directorul **Spam** este creat în timpul instalării Bitdefender.
- În Outlook Express și Windows Mail, mesajele spam sunt mutate direct în **Deleted Items**.
- În Mozilla Thunderbird, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Trash**.Directorul **Spam** este creat în timpul instalării Bitdefender.

Dacă utilizați alt client de mail, trebuie să creați o regulă pentru a muta mesajele e-mail marcate ca `[spam]` de Bitdefenderîntr-un anumit director de carantină.

17.1. Detalii privind modulul Antispam

17.1.1. Filtrele Antispam

Motorul Bitdefender Antispam încorporează mai multe filtre diferite care vă protejează directorul Inbox împotriva mesajelor spam: Lista de prieteni, Lista de spammeri, Filtru de caractere, Filtru de link-uri, Filtru de semnături, Filtru NeuNet (Heuristic) și detecție in-the-cloud.

Lista de prieteni/Lista de spanmmeri

Majoritatea oamenilor comunică în mod regulat cu un grup de cunoștințe sau chiar primesc mesaje de la companii sau organizații cu același domeniu de activitate. Prin utilizarea **listei de prieteni sau de spammeri**, puteți clasifica ușor persoanele de la care doriți să primiți e-mail-uri (prieteni) indiferent de conținutul mesajului sau persoanele de la care nu mai doriți să primiți deloc mesaje (spammeri).

Notă

Vă recomandăm să adăugați numele și adresele prietenilor la **Lista de prieteni**. Bitdefendernu blochează mesajele persoanelor aflate în această listă; de aceea, adăugarea prietenilor în listă asigură primirea mesajelor legitime.

Filtrul de caractere

Multe mesaje Spam sunt scrise cu caractere chirilice și / sau asiatice. Filtrul de caractere detectează acest tip de mesaje și le marchează ca SPAM.

Filtrare link-uri

Aproape toate mesajele spam conțin referințe (linkuri) la diverse pagini web. Aceste pagini conțin, de obicei, reclame și oferă posibilitatea de a cumpăra obiecte și, uneori, sunt folosite pentru tentative de phishing.

Bitdefender menține o bază de date cu astfel de linkuri.Filtrul de link-uri verifică fiecare link URL dintr-un mesaj în baza sa de date. Dacă există o concordanță, mesajul este etichetat ca SPAM.

Filtrul semnăturilor

Cercetătorii Bitdefender în materie de spam-uri analizează în mod constant mesajele e-mail de tip spam "in the wild" și lansează semnături spam pentru a permite detectarea acestora.

Filtrul semnăturilor verifică e-mail-urile pe baza semnăturilor spam din baza de date locală.Dacă există o concordanță, mesajul este etichetat ca SPAM.

Notă

Spre deosebire de alte filtre, Filtrul de semnături nu poate fi dezactivat în mod independent de protecția antispam.

Filtrul Euristic

Filtrul NeuNet (euristic) verifică toate componentele unui mesaj, (nu doar antetul, ci și corpul mesajului în format HTML sau text), căutând cuvinte, fraze, linkuri sau alte caracteristici ale spamului.Pe baza rezultatelor analizei, e-mailul va primi un punctaj spam.

Dacă punctajul spam depășește nivelul limită, e-mail-ul este considerat ca fiind SPAM.Nivelul limită este definit prin intermediul nivelului de sensibilitate antispam.Pentru mai multe informații, consultați *„Ajustarea nivelului de sensibilitate” (p. 96)*.

Filtrul detectează, de asemenea, mesajele marcate SEXUALLY-EXPLICIT: în subiect și le marchează ca SPAM.

Notă

Începând din 19 Mai 2004, mesajele Spam care conțin material cu specific sexual trebuie să includă avertismentul SEXUALLY-EXPLICIT: în subiect. În caz contrar expeditorii vor fi acuzați de încălcarea legii și ulterior amendați.

Detecție in-the-cloud

Detecția in-the-cloud folosește serviciile Bitdefender Cloud pentru a vă oferi protecție antispam eficientă și întotdeauna actualizată.

Mesajele e-mail sunt verificate cu ajutorul tehnologiei in the cloud, doar dacă rezultatul filtrelor antispam nu este concludent.

17.1.2. Funcționarea Antispam

Motorul antispam al Bitdefender utilizează concomitent toate filtrele antispam pentru a determina dacă un anumit mesaj e-mail ar trebui să ajungă în directorul **Inbox (Mesaje primite)** sau nu.

Fiecare mesaj e-mail pe care îl primiți este întâi verificat de filtrul Lista de prieteni/Lista de spammeri. Dacă adresa expeditorului se regăsește în Lista de prieteni mesajul este trimis direct în **Inbox**.

În caz contrar, filtrul Lista de spammer-i va verifica dacă adresa expeditorului se află pe această listă. Dacă adresa este găsită, e-mail-ul este etichetat ca SPAM și este mutat în directorul **Spam**.

Altfel, Filtrul de caractere va verifica dacă mesajul este scris cu caractere Chirilice sau Asiatice. În acest caz, e-mail-ul este etichetat ca SPAM și mutat în directorul **Spam**.

Filtrul Link va compara linkurile găsite în e-mail cu cele din colecția de linkuri spam cunoscute a Bitdefender. În cazul unei potriviri, e-mail-ul va fi considerat SPAM.

După aceea, Filtrul semnăturilor verifică e-mail-ul pe baza semnăturilor spam din baza de date locală.Dacă există o concordanță, mesajul este etichetat ca SPAM.

Filtrul NeuNet (euristic) va prelua mesajul și va verifica toate componentele acestuia, căutând cuvinte, fraze, linkuri sau alte caracteristici SPAM. Pe baza rezultatelor analizei, e-mailul va primi un punctaj spam.

Notă
Dacă mesajul este etichetat ca SEXUALLY EXPLICIT în subiect, Bitdefender îl va considera SPAM.

Dacă punctajul spam depășește nivelul limită, e-mail-ul este considerat ca fiind SPAM.Nivelul limită este definit prin intermediul nivelului de protecție antispam.Pentru mai multe informații, consultați *„Ajustarea nivelului de sensibilitate”* (p. 96).

Dacă filtrele locale antispam nu furnizează un rezultat concludent, e-mail-ul este verificat cu ajutorul tehnologiei de detecție in-the-cloud, prin intermediul căreia se ia decizia dacă un e-mail este spam sau legitim.

17.1.3. Actualizări Antispam

De fiecare dată când este efectuată o actualizare, sunt adăugate în bazele de date noi semnături și link-uri pentru e-mail-urile spam cunoscute.Aceasta permite sporirea eficienței motorului Antispam.

Pentru a vă proteja de spammeri, Bitdefender poate realiza actualizări automate. Păstrați opțiunea **Actualizare automatică** activată.

17.1.4. Clienți și protocoale de e-mail compatibile

Protecția antispam este oferită pentru toți clienții de mail POP3/SMTP.Bara de comenzi antispam însă este integrată doar în:

- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express și Windows Mail (pe sisteme de 32 bit)
- Mozilla Thunderbird 3.0.4

17.2. Activarea sau dezactivarea protecției antispam

Protecția antispam nu este activată implicit.Pentru a activa modulul antispam, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antispam**, faceți clic pe butonul de activare sau dezactivare a opțiunii **Antispam**.
3. Așteptați până când Bitdefender instalează componentele modulului.

17.3. Utilizarea barei de instrumente antispam în fereastra de client de e-mail

În partea de sus a ferestrei clientului dumneavoastră de mail, puteți vedea bara de comenzi antispam.Bara de comenzi antispam vă ajută să administrați protecția

antispam direct din clientul dumneavoastră de mail.Puteți corecta Bitdefender cu ușurință dacă acesta a marcat un mesaj legitim ca SPAM.

Important

Bitdefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat.Pentru o listă completă a clienților de mail admiși, consultați *„Clienți și protocoale de e-mail compatibile”* (p. 91).

Fiecare buton al barei de comenzi este explicat mai jos:

Este Spam - indică faptul că mesajul e-mail selectat este spam.Mesajul e-mail va fi mutat imediat în directorul **Spam**.Dacă serviciile antispam cloud sunt activate, mesajul va fi trimis către Bitdefender Cloud pentru a fi analizat în detaliu.

Nu este spam - indică faptul că mesajele e-mail selectate nu sunt de tip spam și Bitdefender nu ar fi trebuit să le eticheteze astfel.E-mailul va fi mutat din directorul **Spam** în directorul **Inbox** (Mesaje primite).Dacă serviciile antispam cloud sunt activate, mesajul va fi trimis către Bitdefender Cloud pentru a fi analizat în detaliu.

Important

Butonul **Nu este Spam** este activ doar când selectați un mesaj etichetat ca SPAM de către Bitdefender (în mod normal aceste mesaje se găsesc în directorul **Spam**).

Adaugă Spammer - adaugă expeditorul e-mailului selectat pe Lista de spammeri.Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare.Mesajele e-mail primite de la adrese de pe Lista de spammeri sunt marcate automat ca `[spam]`.

Adaugă prieten - adaugă expeditorul e-mailului selectat pe Lista de prieteni.Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare.Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.

Spammeri - deschide **lista de spammeri** care conține adrese de e-mail de la care nu doriți să primiți mesaje, indiferent de conținutul acestora.Pentru mai multe informații, consultați *„Configurarea listei de spammeri”* (p. 95).

Prieteni - deschide **lista de prieteni** care conține adrese de e-mail de la care doriți întotdeauna să primiți mesaje, indiferent de conținutul acestora.Pentru mai multe informații, consultați *„Configurarea listei de prieteni”* (p. 94).

Setări - deschide o fereastră în care puteți configura filtrele antispam și setările barei de instrumente.

17.3.1. Indicarea erorilor de detecție

Dacă folosiți un client de e-mail compatibil, puteți corecta cu ușurință filtrul antispam (indicând ce mesaje e-mail nu ar fi trebuit marcate ca fiind de tip `[spam]`). Astfel, veți îmbunătăți eficiența filtrului antispam.Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.

2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele legitime pe care Bitdefender le-a marcat incorect ca `[spam]`.
4. Faceți clic pe butonul **Adaugă prieten** din bara de instrumente antispam Bitdefender, pentru a adăuga expeditorul pe Lista de prieteni.Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare.Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.
5. Faceți clic pe butonul **Nu este spam** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail).Mesajul e-mail va fi mutat în directorul Mesaje primite.

17.3.2. Indicarea mesajelor spam nedetectate

Dacă folosiți un client de mail admis, puteți indica cu ușurință care mesaje e-mail ar fi trebuit detectate ca spam. Astfel, veți îmbunătăți eficiența filtrului antispam.Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți la directorul Inbox.
3. Selectați mesajele spam nedetectate.
4. Faceți clic pe butonul **Spam** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail). Acestea sunt marcate imediat ca `[spam]` și mutate în directorul de mesaje nesolicitate (junk).

17.3.3. Configurarea setărilor barei de instrumente

Pentru a configura setările barei de instrumente antispam pentru clientul de e-mail, faceți clic pe butonul **Setări** din bara de instrumente și apoi pe fila **Setări bară din instrumente**

Setările sunt grupate în două categorii:

- În categoria **Reguli e-mail** aveți posibilitatea de a configura regulile de procesare a mesajelor e-mail de tip spam detectate de Bitdefender.
  - **Mută mesajul la Obiecte șterse** (doar pentru Microsoft Outlook Express / Windows Mail)

Notă
În Microsoft Outlook / Mozilla Thunderbird, mesajele de tip spam detectate sunt mutate automat în directorul Spam, localizat în directorul Elemente șterse / Reciclare.

- **Marchează e-mail-urile spam ca 'citite'** - marchează, în mod automat, mesajele e-mail de tip spam ca fiind citite, astfel încât să nu fiți deranjat la primirea unui astfel de mesaj.

- La categoria **Notificări** puteți alege dacă să fie afișate sau nu ferestrele de confirmare când faceți clic pe butoanele **Adaugă Spammer** și **Adaugă prieten** din bara de instrumente antispam.Ferestrele de confirmare pot preveni adăugarea accidentală a expeditorilor de mesaje e-mail la lista de prieteni/contacte care trimit mesaje spam.

17.4. Configurarea listei de prieteni

Lista de Prieteni este o listă care conține toate adresele de e-mail de la care doriți să primiți mesaje, indiferent de conținutul acestora. Mesajele de la prieteni nu vor fi etichetate ca Spam, chiar dacă au conținut asemănător mesajelor Spam.

Notă
Orice mesaj venit de la o adresă inclusă pe **lista de prieteni** va fi trimis automat în directorul Inbox, fără a mai fi procesat.

Pentru a configura și administra lista de prieteni:

- Dacă utilizați Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, faceți clic pe butonul **Prieteni** de pe bara de instrumente antispam Bitdefender integrată în clientul dumneavoastră de e-mail.

- Alternativ, urmați acești pași:
  1. Deschideți fereastra Bitdefender.
  2. În panoul **Antispam**, faceți clic pe **Administrare** și selectați **Administrare prieteni** din meniul derulant.

Pentru a adăuga o adresă de e-mail, selectați opțiunea **Adresă e-mail**, introduceți adresa și apoi faceți clic pe **Adaugă**.Sintaxă: nume@domeniu.com.

Pentru a adăuga toate adresele de e-mail dintr-un anumit domeniu, selectați opțiunea **Nume domeniu**, introduceți numele domeniului și faceți clic pe **Adaugă**.Sintaxă:

- @domeniu.com, *domeniu.com și domeniu.com - toate mesajele primite de la domeniu.com vor ajunge în directorul **Inbox** indiferent de conținut;
- *domeniu* - toate mesajele primite de la domeniu (indiferent de sufixul domeniului) vor ajunge în directorul **Inbox** indiferent de conținut;
- *com - toate mesajele primite având sufixul domeniului com vor ajunge în directorul **Inbox** indiferent de conținut;

Se recomandă să evitați adăugarea de domenii, însă acest lucru poate fi util în anumite situații.De exemplu, puteți adăuga domeniul de e-mail al companiei pentru care lucrați sau pe cele ale partenerilor dumneavoastră de încredere.

Pentru a șterge un element de pe listă, faceți clic pe link-ul **Elimină** corespunzător.Pentru a șterge toate înregistrările de pe listă faceți clic pe butonul **Șterge lista** și apoi pe **Da**, pentru confirmare.

Puteți salva Lista de prieteni într-un fișier, astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului.Pentru a salva Lista de prieteni, faceți clic pe butonul **Salvează** și salvați-o în locația dorită.Fișierul va avea extensia `.bwl`.

Pentru a încărca o Listă de prieteni salvată anterior, faceți clic pe butonul **Încarcă** și deschideți fișierul `.bwl` corespunzător.Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Suprascrie lista curentă**.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

17.5. Configurarea listei de spammeri

Lista de spammeri este o listă care conține toate adresele de e-mail de la care nu doriți să primiți mesaje, indiferent de conținutul acestora.Orice mesaj primit de la o adresă din **lista de spammeri** va fi automat etichetat ca Spam, fără altă procesare.

Pentru a configura și administra lista de spammeri:

- Dacă utilizați Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, faceți clic pe butonul **Spammeri** de pe bara de instrumente antispam Bitdefender integrată în clientul dumneavoastră de e-mail.
- Alternativ, urmați acești pași:
  1. Deschideți fereastra Bitdefender.
  2. În panoul **Antispam**, faceți clic pe **Administrare** și selectați **Administrare Spammeri** din meniul derulant.
  3. Mergeți la secțiunea **Antispam**
  4. Faceți clic pe **Administrare** și selectați **Spammeri** din meniu.

Pentru a adăuga o adresă de e-mail, selectați opțiunea **Adresă e-mail**, introduceți adresa și apoi faceți clic pe **Adaugă**.Sintaxă: nume@domeniu.com.

Pentru a adăuga toate adresele de e-mail dintr-un anumit domeniu, selectați opțiunea **Nume domeniu**, introduceți numele domeniului și faceți clic pe **Adaugă**.Sintaxă:

- @domeniu.com, *domeniu.com și domeniu.com - toate mesajele primite de la domeniu.com vor fi etichetate ca SPAM;
- *domeniu* - toate mesajele primite de la domeniu (indiferent de sufixul domeniului) vor fi etichetate ca SPAM;
- *com - a- toate mesajele primite având sufixul domeniului com vor fi etichetate ca SPAM.

Se recomandă să evitați adăugarea de domenii, însă acest lucru poate fi util în anumite situații.

Avertisment

Nu adăugați nume de domenii legitime ale unor servicii de e-mail bazate pe web (Yahoo, Gmail, Hotmail sau altele asemenea) pe Lista de spammeri. În caz contrar, mesajele e-mail primite de la orice utilizator înregistrat al unui astfel de serviciu va fi detectat ca spam. Dacă, de exemplu, adăugați `yahoo.com` pe Lista de spammeri, toate mesajele e-mail care provin de la adrese `yahoo.com` vor fi marcate ca `[spam]`.

Pentru a șterge un element de pe listă, faceți clic pe link-ul **Elimină** corespunzător.Pentru a șterge toate înregistrările de pe listă faceți clic pe butonul **Șterge lista** și apoi pe **Da**, pentru confirmare.

Puteți salva Lista de spammeri într-un fișier astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului.Pentru a salva Lista de spammeri, faceți clic pe butonul **Salvează** și salvați-o în locația dorită.Fișierul va avea extensia `.bwl`.

Pentru a încărca o Listă de spammeri salvată anterior, faceți clic pe butonul **Încarcă** și deschideți fișierul `.bwl` corespunzător.Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Suprascrie lista curentă**.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

17.6. Ajustarea nivelului de sensibilitate

În cazul în care observați că mesaje e-mail legitime sunt marcate ca fiind spam sau că multe mesaje e-mail de tip spam trec nedetectate, puteți ajusta nivelul de sensibilitate antispam pentru a încerca să soluționați problema.Totuși, este recomandat să citiți mai întâi *„Filtrul Antispam nu funcționează corespunzător”* (p. 139) și să urmați instrucțiunile pentru a remedia problema, decât să modificați nivelul de sensibilitate în mod independent.

Pentru a ajusta nivelul de sensibilitate amtispa, urmați pașii de mai jos.

1. Deschideți Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentarea setărilor**, selectați **Antispam**.
4. În fereastra **Setări Antispam**, selectați secțiunea **Setări**.
5. Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de sensibilitate care se potrivește mai bine nevoilor dumneavoastră de securitate.Descrierea vă informează, de asemenea, despre orice acțiuni suplimentare pe care ar trebui să le luați pentru a evita potențialele probleme sau pentru a spori eficiența detecției antispam.

17.7. Se configurează filtrele locale antispam

Conform descrierii de la *„Detalii privind modulul Antispam”* (p. 88), Bitdefender utilizează o combinație de diferite filtre antispam pentru a identifica mesajele spam.Filtrele antispam sunt preconfigurate pentru asigurarea unei protecții eficiente.

Important

Dacă primiți e-mailuri legitime scrise cu caractere asiatice sau chirilice, dezactivați setarea care blochează în mod automat aceste e-mailuri.Setarea corespunzătoare este dezactivată pentru versiunile localizate ale programului care utilizează astfel de seturi de caractere (de exemplu, în cazul versiunii în limba rusă sau chineză).

Pentru a configura filtrele locale antispam, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentarea setărilor**, selectați **Antispam**.
4. În fereastra **Setări Antispam**, selectați secțiunea **Setări**.
5. Faceți clic pe comutatoare pentru a activa sau dezactiva filtrele locale antispam.

În cazul în care utilizați Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, puteți configura filtrele locale antispam direct din clientul de e-mail.Faceți clic pe butonul **Setări** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail) și apoi pe fila **Filtre antispam**.

17.8. Configurarea detecției in-the-cloud

Detecția in-the-cloud folosește serviciile Bitdefender Cloud pentru a vă oferi protecție antispam eficiență și întotdeauna actualizată.

Pentru a configura detecția in-the-cloud, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentarea setărilor**, selectați **Antispam**.
4. În fereastra **Setări Antispam**, selectați secțiunea **Cloud**
5. Faceți clic pe comutator pentru a activa sau dezactiva opțiunea de detecție in-the-cloud.
6. Mostre de mesaje e-mail legitime și de tip spam pot fi trimise către Bitdefender Cloud în cazul în care identificați erori de detecție sau mesaje e-mail de tip spam nedetectate. Acest lucru vă ajută să îmbunătățiți rata de detecție antispam a

Bitdefender.Configurați trimiterea mostrelor de e-mail către Bitdefender Cloud, selectând opțiunile dorite.

În cazul în care utilizați Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, puteți configura detecția in-the-cloud direct de la clientul dumneavoastră de e-mail.Faceți clic pe butonul **Setări** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail) și apoi pe fila **Setări Cloud**.

18. Control date

Informațiile dumneavoastră private reprezintă o țintă constantă pentru criminalii cibernetici.Din moment ce amenințările s-au răspândit aproape asupra întregului spectru de activități online, o protecție neadecvată a e-mail-ului, a mesajelor instante și a activităților de navigare pe internet poate duce la scurgeri de informații care vă pot compromite confidențialitatea.

În plus, există posibilitatea ca fișierele stocate pe computerul dumneavoastră să ajungă într-o zi pe mâini greșite.

Opțiunea Control date a Bitdefender cuprinde toate amenințările ce prezintă o multitudine de componente.

- Protecția antiphising - oferă un set complet de caracteristici care vă protejează permanent în timp ce navigați pe internet și, în plus, vă împiedică să oferiți informații personale site-urilor web frauduloase, ce par legitime la prima vedere.
- Criptare mesagerie instant - criptează mesajele instante pentru a vă asigura că conținutul lor rămân între dumneavoastră și partenerul de chat.
- Ștergere definitivă fișier - șterge definitiv fișiere și orice urmă ale acestora din computerul dumneavoastră.

18.1. Protecție antiphishing

Bitdefender Antiphishing împiedică dezvăluirea informațiilor personale în timp ce navigați pe Internet alertându-vă despre paginile web cu conținut potențial phishing.

Bitdefender furnizează protecție antiphishing în timp real pentru:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger

Pentru a configura setările Antiphishing, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Control date**.
4. În fereastra **Setări control date**, selectați secțiunea **Antiphishing**.

Faceți clic pe comutatoare pentru a activa sau dezactiva:

- Afișarea barei de instrumente Bitdefender în browser-ul de web.

Notă
Bara de instrumente pentru browser a Bitdefender nu este activată implicit.

- Asistență pentru căutare, o componentă care clasifică rezultatele căutărilor efectuate cu ajutorul motoarelor de căutare și link-urile publicate în rețelele sociale prin afișarea unei pictograme în dreptul fiecărui rezultat:

  Nu este recomandat să vizitați această pagină web.

  Această pagină web poate avea conținut periculos. Vizitați cu atenție această pagină.

  Această pagină este una sigură.

  Funcția de Asistență pentru căutare clasifică rezultatele generate de următoarele motoare de căutare:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Funcția de Asistență pentru căutare clasifică link-urile publicate pe următoarele site-uri de socializare:
  - Facebook
  - Twitter

- Scanarea traficului web SSL

  Atacurile mai sofisticate pot folosi trafic de web securizat pentru a induce în eroare victimele.Așadar, este recomandat să activați scanarea SSL.

- Protecție împotriva fraudelor.
- Protecție împotriva tentativelor de phishing.
- Protecția mesajelor instante.

Puteți configura o listă de site-uri web care nu vor fi scanate de către motoarele antiphishing Bitdefender.Este recomandat ca lista să conțină doar site-uri web în care aveți deplină încredere.De exemplu, adăugați site-urile web de unde cumpărați produse online.

Pentru a configura și administra lista albă antiphishing, faceți clic pe link-ul **Listă albă**Va apărea o nouă fereastră.

Pentru a adăuga un site pe lista albă, introduceți adresa acestuia în câmpul corespunzător și faceți clic pe **Adăugă**.

Pentru a șterge un site web din listă, selectați-l din listă și faceți clic pe link-ul corespunzător **Ștergere**.

Faceți clic pe **Salvează** pentru a salva modificările și închide fereastra.

18.1.1. Protecție Bitdefender în browser-ul web

Bitdefender se integrează direct, printr-o bară de comenzi intuitivă și ușor de folosit, cu următoarele browsere web:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera

Bara de instrumente Bitdefender nu este aceeași cu bara de instrumente a browser-ului dumneavoastră obișnuit.Singurul lucru pe care îl adaugă browser-ului dumneavoastră este un mic instrument de glisare în partea superioară a fiecărei pagini web.Faceți clic pe acesta pentru a vizualiza bara de instrumente.

Bara de instrumente Bitdefender conține următoarele elemente:

Clasificarea paginii

În funcție de cum este clasificată pagina web pe care o vizualizați în acel moment de către Bitdefender, va fi afișată, în partea stângă a barei de instrumente, una dintre următoarele clasificări:

- Mesajul "Această pagină nu este sigură" este afișat pe fundal roșu - trebuie să părăsiți imediat pagina de internet. Pentru a afla mai multe informații despre această amenințare, faceți clic pe simbolul **+** de la clasificarea paginii.
- Mesajul "Atenție!" este afișat pe un fundal portocaliu - această pagină web poate avea un conținut periculos.Vizitați cu atenție această pagină.
- Mesajul "Această pagină este sigură" este afișat pe fundal verde - aceasta este o pagină securizată pe care o puteți vizita.

Sandbox

Faceți clic pe pentru a lansa browser-ul într-un mediu oferit de Bitdefender, izolându-l de sistemul de operare.În acest fel veți împiedica amenințările ce acționează prin intermediul browser-ului să exploateze vulnerabilitățile browser-ului și să câștige controlul asupra sistemului dumneavoastră.Atunci când vizitați pagini web care credeți că ar putea conține acțiuni periculoase, utilizați Sandbox.

Ferestrele de browser deschise în Sandbox vor fi recunoscute cu ușurință prin conturul modificat și pictograma Sandbox care apare în centrul barei de titlu.

Notă
Sandbox nu este disponibil pe computerele ce rulează pe Windows XP.

Setări

Faceți clic pe pentru a selecta caracteristici individuale, prin intermediul cărora să activați sau să dezactivați:

- Filtru Antiphishing
- Filtru web antimalware
- Asistență pentru căutare

Întrerupător de rețea

Pentru a activa/dezactiva complet caracteristicile barei de instrumente, faceți clic pe , în partea dreaptă a barei de instrumente.

18.1.2. Alertele Bitdefender sunt afișate în browser

De fiecare dată când încercați să vizitați un site web clasificat ca fiind nesigur, acesta este blocat și este deschisă o pagină de avertizare în browser-ul dumneavoastră.

Pagina conține informații precum URL-ul site-ului web și amenințarea detectată.

Trebuie să decideți ce veți face în continuare. Sunt disponibile următoarele opțiuni:

- Navigați în afara paginii făcând clic pe **Revenire la pagina securizată**.
- Dezactivați blocarea paginilor ce pot conține tentative de phishing făcând clic pe **Dezactivare filtru antiphishing**.
- Dezactivați blocarea paginilor ce pot conține programe periculoase făcând clic pe **Dezactivare filtru antimalware**.
- Adăugați pagina la lista albă Antiphishing făcând clic pe **Adaugă pe lista albă**.Pagina nu va mai fi scanată de motoarele Bitdefender Antiphishing.
- Vizitați pagina web în ciuda avertismentului, făcând clic pe **Înțeleg riscurile, vreau să continui oricum**.

18.2. Criptare IM

Conținutul conversațiilor dumneavoastră prin mesagerie instant trebuie să rămână doar între dumneavoastră și interlocutorul dumneavoastră.Prin criptarea conversațiilor, vă puteți asigura că oricine încearcă să vă intercepteze mesajele instant trimise sau primite nu poate citi conținutul acestora.

În mod implicit, Bitdefender criptează toate conversațiile dumneavoastră prin mesagerie instant dacă sunt îndeplinite următoarele condiții:

- Partenerul dumneavoastră de chat are instalată o versiune de Bitdefender care suportă criptarea mesajelor instant, iar criptarea este activată pentru aplicația de mesagerie instant folosită pentru chat.
- Dumneavoastră și partenerul dumneavoastră de chat folosiți Yahoo! Messenger.

Important
Bitdefender nu va cripta o conversație dacă unul dintre partenerii de chat folosește o aplicație online pentru chat, cum ar fi Meebo.

Odată ce condițiile preliminare au fost îndeplinite, Bitdefender vă va informa cu privire la starea de criptare a sesiunii de chat prin intermediul unor mesaje afișate în fereastra de chat.

Pentru a activa sau dezactiva criptarea mesajelor instant, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Control date**.
4. În fereastra **Setări control date**, faceți clic pe buton pentru a activa sau dezactiva criptarea mesajelor instant. Criptarea este activată în mod implicit.

18.3. Ștergerea permanentă a fișierelor

Atunci când ștergeți un fișier, acesta nu mai poate fi accesat prin mijloace normale. Cu toate acestea, fișierul continuă să existe pe hard disc până ce este suprascris prin copierea altor fișiere.

Opțiunea de ștergere definitivă a fișierelor oferită de Bitdefender vă va ajuta să ștergeți definitiv date prin eliminarea fizică a acestora de pe hard disk.

Puteți șterge definitiv și rapid fișiere și directoare din computerul dumneavoastră, cu ajutorul meniul contextual Windows, urmând pașii de mai jos:

1. Faceți clic dreapta pe un fișier sau director pe care doriți să-l ștergeți definitiv.
2. Selectați **Bitdefender** > **Ștergere definitivă fișiere** din meniul contextual afișat.
3. Va apărea o fereastră de configurare.Faceți clic pe **Da** pentru a porni asistentul Ștergere definitivă fișiere.
4. Așteptați ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.
5. Sunt afișate rezultatele.Faceți clic pe **Închide** pentru a părăsi asistentul.

Ca alternativă, puteți șterge definitiv fișierele din interfața Bitdefender.

1. Deschideți fereastra Bitdefender.
2. În panoul **Control date**, faceți clic pe **Securitate** și selectați **Ștergere definitivă fișiere** din meniul derulant.
3. Urmați pașii asistentului de ștergere definitivă a fișierelor:
   a. **Selectează fișier/director**

      Adăugați fișierele sau directoarele pe care doriți să le ștergeți definitiv.

b. **Șterge definitiv fișiere**

Așteptați ca Bitdefender să finalizeze ștergerea definitivă a fișierelor.

c. **Rezultate**

Sunt afișate rezultatele.Faceți clic pe **Închide** pentru a părăsi asistentul.

19. Firewall

Firewall-ul vă protejează calculatorul contra tentativelor de conectare interne și externe neautorizate, atât în rețele locale, cât și pe Internet.Este asemănător unui paznic - ține evidența tentativelor de conectare și decide pe care să le permite și pe care să le blocheze.

Firewall-ul Bitdefender folosește un set de reguli pentru a filtra datele transmise către și de la sistemul dumneavoastră.Regulile sunt grupate în 3 categorii:

Reguli generale
: Reguli care determină protocoalele pe care este permisă comunicarea.

  Este utilizat un set de reguli implicite care oferă o protecție optimă.Puteți edita regulile permițând sau respingând conexiunile față de anumite protocoale.

Reguli privind aplicația
: Reguli care determină modul în care fiecare aplicație poate accesa internetul și resursele rețelei.

  În condiții normale, Bitdefender creează în mod automat o regulă de fiecare dată când o aplicație încearcă să acceseze internetul.De asemenea, puteți edita sau adăuga manual reguli pentru aplicații.

Reguli adaptor
: Regulile care determină în ce măsură este posibilă comunicarea dintre calculatorul dumneavoastră și alte calculatoare conectate la aceeași rețea.

  Trebuie să creați reguli pentru a permite în mod specific sau a respinge calculatorul dumneavoastră sau alte calculatoare.

În cazul în care calculatorul dumneavoastră rulează Windows Vista sau Windows 7, Bitdefender alocă automat un nou tip fiecărei conexiuni la rețea detectate.În funcție de tipul de rețea, protecția firewall este setată la nivelul corespunzător pentru fiecare conexiune.

Pentru a afla mai multe despre setările firewall pentru fiecare tip de rețea și despre modul în care puteți edita setările rețelei, consultați *„Administrarea setărilor de conectare”* (p. 106).

Este furnizată protecție suplimentară prin intermediul Sistemului de detecție a intruziunilor (IDS).Sistemul de detectare a intruziunilor monitorizează activitatea rețelei și a sistemului pentru a detecta activități periculoase sau încălcări ale politicii.Poate, de asemenea, detecta și bloca tentativele de modificare a fișierelor de sistem importante, a fișierelor Bitdefender sau a intrărilor de regiștri, instalarea de drivere periculoase și atacurile realizate prin injectarea de coduri (injectare DLL).

Bitdefender este configurat, în mod implicit să aplice automat acțiunile necesare pentru protecția dumneavoastră, fără a vă deranja.Dacă doriți să fiți la curent și să decideți dumneavoastră care este cea mai bună acțiune atunci când o aplicație

solicită accesul la internet sau prezintă semne de comportament suspect, trebuie să activați Paranoid Mode.

19.1. Activarea sau dezactivarea protecției firewall.

Pentru a activa sau dezactiva protecția firewall, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Firewall**, faceți clic pe butonul Firewall.

Avertisment

Deoarece vă expune computerul unor conexiuni neautorizate, dezactivarea firewallului trebuie să fie doar o măsură temporară.Reactivați firewall-ul cât mai repede posibil.

19.2. Administrarea setărilor de conectare

Pentru a vizualiza și edita setările conexiunii rețelei, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Firewall**, faceți clic pe **Administrare adaptoare**.

Va apărea o nouă fereastră.Graficul din partea superioară a ferestrei prezintă informații în timp real privind traficul recepționat și trimis.

Următoarele informații sunt afișate sub grafic pentru fiecare conexiune la rețea.

- **Tip rețea** - tipul de rețea la care este conectat computerul dumneavoastră.Bitdefender aplică un set de bază de setări firewall în funcție de tipul de rețea la care sunteți conectat.

  Puteți modifica tipul deschizând meniul vertical **Tip de rețea** și selectând unul dintre tipurile disponibile din listă.

Tip rețea	Descriere
Sigură	Dezactivează firewallul pentru adaptorul respectiv.
Acasă/Serviciu	Permite tot traficul dintre calculatorul dumneavoastră și calculatoarele din rețeaua locală.
Public	Tot traficul este filtrat.
Nesigură	Blochează complet traficul de rețea și Internet prin adaptorul respectiv.

- **Mod ascuns** - dacă puteți fi detectat de alte calculatoare.

  Pentru a configura modul Stealth, selectați opțiunea dorită din meniul derulant corespunzător.

Opțiune	Descriere
Activ	Modul ascuns este activat.Computerul dumneavoastră nu poate fi detectat nici din rețeaua locală, nici de pe internet.
Inactiv	Modul ascuns este dezactivat.Oricine din rețeaua locală sau de pe Internet poate da ping și detecta calculatorul dumneavoastră.
La distanță	Calculatorul dumneavoastră nu poate fi detectat din Internet.Utilizatorii din rețeaua locală pot da ping și detecta calculatorul dumneavoastră.

- **Generic** - dacă sunt aplicate reguli generice pentru această conexiune.

  Dacă se schimbă adresa IP a unui adaptor de rețea, Bitdefender va modifica automat și tipul de rețea.Dacă doriți să mențineți același tip, selectați **Da** din meniul derulant corespunzător.

19.3. Administrarea regulilor firewall

19.3.1. Reguli generale

De fiecare dată când sunt transmise date prin interne, sunt folosite anumite protocoale.

Regulile generale vă permit să configurați protocoalele pe care este permis traficul.Pentru a edita regulile, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Firewall**.
4. În fereastra **Setări firewall**, selectați secțiunea **Setări**.
5. Sub Reguli firewall, faceți clic pe **Reguli generale**.

Va apărea o nouă fereastră.Sunt afișate regulile curente.

Pentru a edita o regulă, faceți clic pe săgeata corespunzătoare din coloana **Acțiune** și selectați **Permite** sau **Respinge**.

DNS față de UDP / TCP
Permite sau respinge DNS față de UDP și TCP.

În mod implicit, acest tip de conexiune este permis.

ICMP / ICMPv6 în curs de recepționare
Permite sau respinge mesajele ICMP / ICMPv6.

Mesajele ICMP sunt folosite adesea de hackeri pentru a lansa atacuri asupra rețelelor computerului.În mod implicit, acest tip de conexiune nu este permis.

Trimiterea mesajelor e-mail
Permite sau respinge trimiterea de mesaje e-mail prin SMTP.

În mod implicit, acest tip de conexiune este permis.

Navigare internet HTTP
Permite sau respinge navigare web HTTP.

În mod implicit, acest tip de conexiune este permis.

Conexiuni desktop de la distanță în curs de recepționare
Permite sau respinge accesul altor computere la conexiunile desktop de la distanță.

În mod implicit, acest tip de conexiune este permis.

Trafic Windows Explorer pe HTTP / FTP
Permite sau respinge traficul HTTP sau FTP de la Windows Explorer.

În mod implicit, acest tip de conexiune nu este permis.

19.3.2. Reguli privind aplicațiile

Pentru a vizualiza și a administra regulile pentru firewall, ce controlează accesul aplicațiilor la resursele rețelei și la internet, faceți clic pe **Reguli aplicație**.

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Firewall**.
4. În fereastra **Setări firewall**, selectați secțiunea **Setări**.
5. Sub Reguli Firewall faceți clic pe **Reguli aplicație**.

Puteți vedea în tabel programele (procesele) pentru care au fost create reguli firewall.Pentru a vedea regulile create pentru o anumită aplicație, faceți clic pe căsuța cu + de lângă aplicația respectivă, sau, pur și simplu, faceți dublu clic pe aplicație.

Pentru fiecare regulă sunt afișate următoarele informații:

- **Proces/Tipuri rețea** - procesul și tipul de adaptor de rețea cărora li se aplică regula.Regulile sunt create automat pentru a filtra accesul la rețea sau Internet prin oricare adaptor.Pentru a filtra accesul aplicațiilor la rețea și Internet printr-un anumit adaptor (de exemplu, printr-un adaptor de rețea wireless), puteți crea reguli manual sau puteți edita regulile existente.
- **Protocol** - protocolul IP căruia i se aplică regula.Puteți vedea unul dintre următoarele protocoale:

Protocol	Descriere
Oricare	Include toate protocoalele IP.
TCP	TCP, acronimul pentru Transmission Control Protocol, permite stabilirea unei conexiuni și schimbul de date între două sisteme. TCP garantează livrarea de date și primirea pachetelor trimise în aceeași ordine în care au fost expediate.
UDP	UDP, acronimul pentru User Datagram Protocol, este un protocol bazat pe IP, proiectat pentru performanțe ridicate. Jocurile și alte aplicații video folosesc adesea acest protocol.
Un număr	Reprezintă un anumit protocol IP (altul decât TCP și UDP).Puteți găsi lista completă a numerelor atribuite protocoalelor IP la adresa http://www.iana.org/assignments/protocol-numbers.

- **Acțiune** - dacă aplicației îi este permis sau nu accesul la rețea sau la internet în circumstanțele date.

Pentru a administra regulile, folosiți butoanele din partea inferioară a ferestrei:

- **Adaugă regulă** - deschide fereastra Adaugă regulă aplicație unde puteți crea o nouă regulă.
- **Editare regulă** - deschide fereastra Editare regulă aplicație în care puteți modifica setările pentru o regulă selectată.
- **Șterge regulă** - șterge regula selectată.

Adăugarea/Editarea regulilor pentru aplicații

Pentru a adăuga sau edita o regulă privind aplicația, faceți clic pe butonul corespunzător.Va apărea o nouă fereastră. Procedați astfel:

- **Cale program.** Faceți clic pe **Caută** și selectați aplicația căreia i se aplică regula.
- **Adresă locală.** Specificați adresa IP locală și portul local cărora li se aplică regula.Dacă aveți mai multe adaptoare de rețea, puteți debifa căsuța **Oricare** și introduce o anumită adresă IP.
- **Adresă remote.** Specificați adresa IP și portul la distanță cărora li se aplică regula.Pentru a filtra traficul dintre calculatorul dumneavoastră și un anumit calculator, debifați căsuța **Oricare** și introduceți adresa IP a acestuia.
- **Tip rețea.** Selectați tipul de rețea pentru care se aplică regula.
- **Evenimente.** În funcție de protocolul selectat, alegeți evenimentele de rețea cărora li se aplică regula.Pot fi luate în considerare următoarele evenimente:

Eveniment	Descriere
Conectare	Schimb preliminar de mesaje standard utilizate în cadrul protocoalelor orientate pe conexiune pentru a stabili o conexiune.În cazul protocoalelor orientate pe conexiune, traficul de date dintre două calculatoare apare numai după ce a fost stabilită conexiunea.
Trafic	Schimb de date dintre două calculatoare.
Ascultă	Stare în care o aplicație monitorizează rețeaua așteptând stabilirea unei conexiuni sau recepționarea unor informații de la o aplicație parteneră.

- **Protocol.** Selectați din meniu protocolul IP căruia i se aplică regula.
  - Dacă doriți ca regula să fie aplicată tuturor protocoalelor, selectați **Oricare**.
  - Dacă doriți ca regula să fie aplicată pentru TCP, selectați **TCP**.
  - Dacă doriți ca regula să fie aplicată pentru UDP, selectați **UDP**.
  - Dacă doriți ca regula să fie aplicată unui anumit protocol, selectați **Altul**.Va apărea un câmp editabil.Introduceți în câmpul editabil numărul atribuit protocolului care doriți să fie filtrat

Notă

Numerele protocoalelor IP sunt atribuite de către Internet Assigned Numbers Authority (IANA).Puteți găsi lista completă a numerelor atribuite protocoalelor IP la adresa http://www.iana.org/assignments/protocol-numbers.

- **Direcție.** Selectați din meniu direcția traficului căreia i se aplică regula.

Direcție	Descriere
La ieșire	Regula nu se va aplica decât pentru traficul la ieșire.
La intrare	Regula nu se aplica decât pentru traficul la intrare.
Ambele	Regula se va aplica în ambele direcții.

- **Versiune IP.** Selectați din meniu versiunea IP (IPv4, IPv6 sau ambele) căreia i se aplică regula.
- **Permisiune.** Selectați una dintre permisiunile disponibile:

Permisiune	Descriere
Permite	Aplicației specificate îi va fi permis accesul la rețea / Internet în condițiile specificate.

Permisiune	Descriere
Interzice accesul	Aplicației specificate îi va fi refuzat accesul la rețea / Internet în condițiile specificate.

19.3.3. Reguli adaptor

Pentru fiecare conexiune la rețea puteți configura zone speciale sigure și nesigure.

O zonă sigură reprezintă un dispozitiv în care aveți încredere deplină, ca de exemplu un computer sau o imprimantă.Este permis în întregime traficul dintre computerul dumneavoastră și un dispozitiv de încredere.Pentru a putea partaja resurse cu calculatoare din rețele fără fir (wireless) nesecurizate, adăugați-le ca fiind calculatoare permise.

O zonă nesigură reprezintă un dispozitiv care nu doriți să comunice sub nicio formă cu computerul dumneavoastră.

Pentru a vizualiza și gestiona zonele de pe adaptorii rețelei dumneavoastră, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Firewall**.
4. În fereastra **Setări firewall**, selectați secțiunea **Setări**.
5. Sub Reguli Firewall faceți clic pe **Reguli adaptor**.

Va apărea o nouă fereastră în care vor fi afișate toate adaptoarele de rețea cu conexiuni active și zonele curente, dacă există.

Pentru a administra zonele, folosiți butoanele din partea inferioară a ferestrei:

- **Adăugare zonă** - deschide fereastra Adăugare adresă IP în care puteți crea o nouă zonă pentru un adaptor selectat.
- **Editare zonă** - deschide fereastra Editare regulă în care puteți modifica setările pentru o zonă selectată.
- **Șterge secțiune** - șterge secțiunea selectată.

Adăugarea / editarea zonelor

Pentru a adăuga sau edita o zonă, faceți clic pe butonul corespunzător.Va apărea o nouă fereastră în care vor fi afișate adresele IP ale dispozitivelor conectate la rețea.Procedați astfel:

1. Selectați adresa de IP a computerului pe care doriți să-l adăugați sau introduceți o adresă sau un interval de adrese în căsuța corespunzătoare.

2. Selectați acțiunea:
   - **Permite** - pentru a permite tot traficul dintre calculatorul dumneavoastră și calculatorul selectat.
   - **Blochează** - pentru a bloca tot traficul dintre calculatorul dumneavoastră și calculatorul selectat.
3. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

19.4. Monitorizarea activității rețelei

Pentru a monitoriza activitatea actuală din rețea/internet (în TCP și UDP) organizată în funcție de aplicație și pentru a deschide jurnalul de firewall Bitdefender, urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Firewall**.
4. În fereastra **Setări firewall**, selectați secțiunea **Avansat**.
5. În Activivitate rețele, faceți clic pe **Activitate rețea**.

Va apărea o nouă fereastră.Puteți vedea traficul total, sortat după aplicație. Pentru fiecare aplicație, puteți vedea conexiunile și porturile deschise, precum și statistici referitoare la viteza traficului la intrare & ieșire și cantitatea de date trimise / primite.

Pentru fiecare conexiune este afișată o pictogramă.Semnificația iconițelor este după cum urmează:

- Indică o conexiune la ieșire.
- Indică o conexiune la intrare.
- Indică un port deschis pe calculatorul dumneavoastră.

Fereastra prezintă, în timp real, activitatea curentă pe rețea / Internet. Pe măsură ce sunt închise conexiuni și porturi, statisticile corespunzătoare acestora dispar treptat.Același lucru se întâmplă tuturor statisticilor unei aplicații care generează trafic sau are porturi deschise atunci când o închideți.

Pentru o listă completă a evenimentelor referitoare la activitatea modulului Firewall (activare/dezactivare firewall, blocare trafic, modificare setări) sau generate de activitățile detectate de firewall (scanare de porturi, blocare tentative de conectare sau trafic conform regulilor), accesați fișierul jurnal al Bitdefender Firewall făcând clic pe **Afișează jurnal**.Locația fișierului jurnal este `?\Program Files\Common Files\Bitdefender\Bitdefender Firewall\bdfirewall.txt`.

19.5. Configurarea intensității alertei

Bitdefender Internet Security 2013 a fost creat să deranjeze cât mai puțin posibil.În condiții normale, nu sunteți nevoit să luați decizii privind permiterea sau respingerea conexiunilor sau acțiunilor pe care le lansează anumite aplicații ce rulează pe sistemul dumneavoastră.Bitdefender ia toate deciziile în locul dumneavoastră.

Dacă doriți să dețineți controlul deplin și să luați dumneavoastră toate deciziile, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Firewall**.
4. În fereastra **Setări firewall**, selectați secțiunea **Setări**.
5. Activați **Paranoid Mode** făcând clic pe selectorul corespunzător.

Notă
Dacă ați activat modul Paranoid, funcția Autopilot este dezactivată automat.

Atâta timp cât Paranoid Mode este activat, se va afișa o alertă care vă va solicita intervenția de fiecare dată când apare una dintre următoarele situații:

- O aplicație încearcă să se conecteze la internet.
- O aplicație încearcă să efectueze o acțiune considerată a fi periculoasă de către Sistemul de detecție a intruziunilor sau de Active Virus Control.

Alerta conține informații detaliate cu privire la aplicație și la comportamentul detectat.Trebuie să selectați fie **Permite** fie **Respinge** în cazul acțiunii cu ajutorul butonului corespunzător.

19.6. Configurarea setărilor avansate

Pentru a configra setările de firewall avansate, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Firewall**.
4. În fereastra **Setări firewall**, selectați secțiunea **Avansat**.

19.6.1. Sistem de detectare a intruziunilor

Pentru a configura sistemul de detecție a intruziunilor, urmați acești pași:

1. Pentru a porni Sistemul de detecție a intruziunilor, faceți clic pe selectorul corespunzător.

2. Trageți de cursor de-a lungul scalei pentru a seta nivelul de agresivitate dorit.Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul care se potrivește mai bine nevoilor dumneavoastră de securitate.

Puteți verifica ce aplicații au fost detectate de Sistemul de detecție a intruziunilor în fereastra Evenimente.

Dacă există aplicații în care aveți încredere și care nu doriți să fie scanate de Sistemul de detecție a intruziunilor, puteți adăuga reguli de excludere pentru acestea.Pentru a exclude o aplicație de la scanare, urmați pașii descriși în secțiunea *„Administrarea proceselor excluse”* (p. 83).

Notă

Funcționarea Sistemului de detectare a intruziunilor este strict legată de funcționarea Active Virus Control.Regulile de excludere a anumitor procese se aplică în cazul ambelor sisteme.

19.6.2. Alte setări

Funcțiile de mai jos pot fi activate sau dezactivate.

- **Partajarea conexiunii Internet** - permite Partajarea conexiunii Internet.

  Notă

  Această opțiune nu activează automat opțiunea de **Partajare a conexiunii Internet** pe sistemul dumneavoastră, ci permite doar acest tip de conexiune dacă îl activați din sistemul dumneavoastră de operare.

- **Blochează scanările de porturi** - detectează și blochează tentativele de a descoperi care porturi sunt deschise.

  Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe calculatorul dumneavoastră.Dacă este detectat un port vulnerabil, aceștia pot pătrunde în calculatorul dumneavoastră.

- **Mărește numărul de cuvinte dintr-un jurnal** - crește numărul de cuvinte folosite într-un jurnal pentru Firewall.

  Bitdefender păstrează un jurnal al evenimentelor referitoare la activitatea modulului Firewall (activare/dezactivare firewall, blocare trafic, modificare setări) sau generate de activitățile detectate de firewall (scanare porturi, blocare tentative de conectare sau trafic conform regulilor).Jurnalul poate fi accesat de la fereastra **Activitate Firewall**, făcând clic pe **Afișează jurnal**.

- **Monitorizare conexiuni Wi-Fi** - atunci când sunteți conectat la rețele wireless, sunt afișate informații privind anumite evenimente de rețea (de exemplu, atunci când un nou computer a fost introdus în rețea).

20. Tranzacții sigure online cu Safepay

Calculatorul a început să devină instrumentul preferat pentru cumpărături și tranzacții bancare. Achitarea facturilor, transferul de bani, achiziționarea a cam tot ce vă puteți imagina nu au fost niciodată mai rapide sau mai ușoare.

Aceasta implică transmiterea de informații personale, date de cont și credit, parole și alte tipuri de informații personale prin Internet, cu alte cuvinte, exact tipul de informații pe care infractorii cibernetici sunt foarte interesați să le obțină. Hackerii se străduiesc în permanență să sustragă aceste informații, deci, nu puteți fi niciodată suficient de precauți cu privire la securizarea tranzacțiilor online.

Bitdefender Safepay oferă o soluție unificată pentru diferitele modalități în care pot fi compromise datele dumneavoastră personale. Acesta este un browser protejat, un mediu securizat, menit să mențină confidențialitatea și siguranța tranzacțiilor dumneavoastră bancare, de cumpărături online sau de alt tip. Puteți lansa Bitdefender Safepay ori de câte ori doriți să transmiteți informații sensibile prin Internet sau îl puteți configura pentru a se activa automat cânt vizitați anumite site-uri Internet.

Bitdefender Safepay oferă următoarele funcții:

- Blochează accesul la calculatorul dumneavoastră și orice încercări de a realiza capturi ale ecranului dumneavoastră.
- Include o tastatură virtuală care, dacă este utilizată, nu permite hackerilor să citească ceea ce introduceți de pe aceasta.
- Este complet idependentă de celelalte browsere ale dumneavoastră.
- Include protecție pentru punctele wireless de acces la Internet încorporată pe care o puteți utiliza în cazul conectării la rețele Wi-fi nesecurizate.
- Acceptă marcajele și vă permite să navigați pe site-urile dumneavoastră preferate de tranzacții bancare/cumpărături.
- Nu se limitează la tranzacții bancare și cumpărături online. Puteți deschide orice site cu Bitdefender Safepay.

20.1. Utilizarea Bitdefender Safepay

În mod implicit, Bitdefender detectează dacă navigați către un site de tranzacții online sau de cumpărături online în orice browser de pe calculatorul dumneavoastră și vă solicită să îl lansați în Bitdefender Safepay.

Pentru a deschide manual Bitdefender Safepay, urmați calea următoare: **Start** → **Toate programele** → **Bitdefender 2013** → **Bitdefender Safepay** sau, mai rapid, faceți dublu clic pe comanda rapidă Bitdefender Safepay de pe calculatorul dumneavoastră.

Dacă sunteți obișnuiți cu browserele Internet, nu veți avea probleme în utilizarea Bitdefender Safepay - arată și se comportă ca un browser obișnuit:

- introduceți URL-urile pe care doriți să le accesați în bara de adrese.
- adăugați secțiuni pentru a accesa mai multe site-uri în fereastra Bitdefender Safepay făcând clic pe .
- reveniți la navigarea anterioară, mergeți către o altă pagină și reîmprospătați pagini folosind .
- accesați setările Bitdefender Safepay făcând clic pe .
- administrați marcajele făcând clic pe de lângă bara de adrese.
- activați tastatura virtuală făcând clic pe .

20.2. Configurarea setărilor

Faceți clic pe pentru a configura următoarele setări:

Comportamentul general Bitdefender Safepay

Selectați ce se va deschide când accesați un site de cumpărături online sau de tranzacții bancare prin Internet, în browserul dumneavoastră Internet obișnuit:

- Deschide automat în Bitdefender Safepay.
- Setați Bitdefender să vă interogheze cu privire la acțiuni de fiecare dată.
- Nu utiliza niciodată Bitdefender Safepay pentru pagini vizitate într-un browser obișnuit.

Listă domenii

Selectați cum se va comporta Bitdefender Safepay la vizitarea site-urilor Internet de pe anumite domenii în browserul dumneavoastră Internet obișnuit, adăugându-le la lista domeniilor și selectând comportamentul fiecăruia dintre ele.

- Deschide automat în Bitdefender Safepay.
- Setați Bitdefender să vă interogheze cu privire la acțiuni de fiecare dată.
- Nu utiliza niciodată Bitdefender Safepay la accesarea unei pagini din domeniu într-un browser obișnuit.

20.3. Administrarea marcajelor

Dacă ați dezactivat detectarea automată a unei părți dintre site-uri sau a tuturor site-urilor sau dacă Bitdefender pur și simplu nu detectează anumite site-uri internet, puteți adăuga marcați în Bitdefender Safepay pentru a putea lansa cu ușurință site-urile Internet în viitor.

Urmați pașii de mai jos pentru a adăuga un URL la marcajele Bitdefender Safepay:

1. Faceți clic pe  de lângă bara de adrese pentru a deschide pagina Marcaje.

   
   Notă
   Pagina Marcaje se deschide în mod implicit la lansarea Bitdefender Safepay.

2. Faceți clic pe butonul **+** pentru a adăuga un marcaj nou.
3. Introduceți URL-ul și titlul marcajului și faceți clic pe **Creează**. URL-ul este și el adăugat la lista Domeniilor de pe pagina setări.

20.4. Protecție pentru punctele wireless de acces la Internet în rețele nesecurizate

Dacă utilizați Bitdefender Safepay în timp ce sunteți conectat la rețele Wi-fi nesecurizate (de exemplu, un punct de acces Internet wireless public) vi se oferă un nivel suplimentar de securizate prin funcția de protecție Hotspot. Acest serviciu criptează comunicarea pe Internet între conexiunile nesecurizate, ajutându-vă să vă mențineți confidențialitatea, indiferent de rețeaua la care sunteți conectat.

Următoarele cerințe preliminare trebuie îndeplinite pentru ca protecția Hotspot să funcționeze:

- Sunteți conectat la MyBitdefender din Bitdefender Internet Security 2013
- Calculatorul dumneavoastră este conectat la o rețea nesecurizată.

După îndeplinirea cerințelor preliminare, Bitdefender vă va interoga automat dacă se utilizează conexiunea securizată, ori de câte ori deschideți Bitdefender Safepay. Nu trebuie decât să introduceți datele de autentificare MyBitdefender atunci când vi se solicită acest lucru.

Conexiunea securizată va fi inițiată și se va afișa un mesaj în fereastra Bitdefender Safepay după conectare. Simbolul  se afișează în fața URL-ului în bara de adrese pentru a vă ajuta să identificați cu ușurință conexiunile securizate.

21. Control Parental

Funcția de Control parental vă permite să controlați accesul la Internet și la anumite aplicații pentru fiecare utilizator care deține un cont de utilizator pe sistem.

După ce ați configurat funcția de Control parental, puteți afla cu ușurință activitățile copiilor dumneavoastră la calculator.

Tot ce vă trebuie este un calculator cu conexiune la internet și un browser web.

Puteți configura funcția de Control parental astfel încât să blocheze:

- pagini web inadecvate.
- accesul la Internet, pentru anumite intervale de timp (de exemplu, în timpul rezervat lecțiilor).
- jocuri, aplicații de chat, partajare de fișiere și altele.
- mesaje instant trimise de alte contacte de mesagerie instant decât cele permise.

Verificați activitatea copiiilor dumneavoastră și modificați setările de Control Parental folosind MyBitdefender de la orice calculator sau dispozitiv mobil conectat la Internet.

21.1. Accesarea panoului funcției de Control parental

Panoul funcției de Control parental este organizat în module, cu ajutorul cărora puteți monitoriza activitățile copilului dumneavoastră pe calculator.

Bitdefender vă permite să controlați accesul la Internet și la aplicațiile specifice pentru copiii dumneavoastră. În același timp, vă permite să le monitorizați activitatea contului de Facebook.

Prin intermediul Bitdefender puteți accesa setările funcției de Control parental din MyBitdefender de la orice calculator sau dispozitiv mobil conectat la Internet.

Accesați-vă contul online:

- Pe orice dispozitiv cu acces la Internet:
  1. Deschideți un browser web.
  2. Mergeți la:https://my.bitdefender.com
  3. Conectați-vă la contul dumneavoastră cu ajutorul numelui de utilizator și parolei.
  4. Faceți clic pe **Control Parental** pentru a accesa panoul de control.
- Din interfața Bitdefender 2013:
  1. Asigurați-vă că sunteți conectat la calculator pe contul de administrator. Doar utilizatorii cu drepturi administrative pe sistem (administratorii de sistem) pot accesa și configura Controlul parental.
  2. Deschideți fereastra Bitdefender.

3. Faceți clic pe butonul **MyBitdefender** din partea de sus a ferestrei și selectați **Control Parental** din meniul derulant.
4. Panoul de Control Parental se va deschide într-o nouă fereastră. Aici puteți verifica și configura setările opțiunii Control parental pentru fiecare cont de utilizator Windows.

21.2. Adăugarea profilului pentru copilul dumneavoastră

Înainte de a configura funcția de Control parental, creați conturi de utilizator Windows separate ce vor fi utilizate de copii. Acestea vă vor permite să știți exact ce face fiecare pe computer. Trebuie să creați conturi de utilizator limitate (standard) pentru ca aceștia să nu poată modifica setările de Control parental. Pentru mai multe informații, consultați *„Cum creez conturi de utilizator Windows?”* (p. 52).

Pentru a adăuga un profil pentru copilul dumneavoastră în modulul de Control parental:

1. Accesați panoul de Control parental direct din contul MyBitdefender.
2. Faceți clic pe **Adăugare copil** în meniul din stânga.
3. Introduceți numele și vârsta copilului în secțiunea **Profil**. Setarea vârstei copilului va încărca automat setările considerate adecvate pentru respectiva categorie de vârstă, pe baza standardelor de dezvoltare a copilului.
4. Selectați secțiunea **Dispozitive**.

   În secțiunea Dispozitive, puteți vizualiza calculatoarele și dispozitivele mobile care sunt asociate contului dumneavoastră MyBitdefender.
5. Selectați calculatorul și contul Windows al copilului dumneavoastră.
6. Faceți clic pe **Salvează**.

   Calculatorul și contul Windows al copilului dumneavoastră sunt acum asociate la contul MyBitdefender.

21.2.1. Monitorizarea activității copilului

Bitdefender vă ajută să urmăriți exact ce face copilul dumneavoastră la calculator.

În acest mod, puteți întotdeauna afla exact ce website-uri au vizitat, ce aplicații au utilizat, sau ce activități au fost blocate de către funcția de Control parental.

Rapoartele conțin informații detaliate pentru fiecare eveniment, cum ar fi:

- Starea evenimentului.
- Numele site-ului blocat.
- Numele aplicației blocate.
- Numele dispozitivului.

- Data și ora producerii evenimentului.
- Acțiunile întreprinse de Bitdefender.

Pentru a monitoriza traficul pe Internet, aplicațiile accesate sau activitatea pe Facebook a copilului dumneavoastră, urmați pașii de mai jos:

1. Accesați panoul de Control parental direct din contul MyBitdefender.
2. Faceți clic pe pentru a accesa fereastra de activități pentru modulul corespunzător.

21.2.2. Configurarea notificărilor prin e-mail

În mod implicit, atunci când funcția de Control parental este activată, activitățile copiilor dumneavoastră sunt înregistrate în fișiere jurnal.

Pentru a primi notificări prin e-mail, urmați pașii de mai jos:

1. Accesați panoul de Control parental direct din contul MyBitdefender.
2. Faceți clic pe pictograma **Setări Generale** din colțul din dreapta sus.
3. Introduceți adresa de e-mail la care vor fi trimise notificările de e-mail.
4. Faceți clic pe butonul de lângă **Actualizare** și reglați frecvența: zilnic, săptămânal sau lunar.

21.3. Configurarea funcției de Control parental

De la panoul funcției de Control parental puteți gestiona în mod direct modulele de Control parental.

Fiecare modul conține următoarele elemente: denumirea modulului, un mesaj de stare, pictograma modulului și un buton care vă permite să efectuați sarcini importante legate de acest modul.

Faceți clic pe o filă pentru a configura funcția corespunzătoare de Control parental pentru calculator:

- Web - pentru a filtra navigarea online și pentru a seta restricții de timp pentru accesarea Internetului
- Aplicații - pentru a bloca sau restricționa accesul la anumite aplicații.
- Facebook - pentru protejarea contului de Facebook al copilului dumneavoastră.
- Mesagerie Instant - acceptarea sau blocarea conversațiilor cu anumite contacte de mesagerie instant.

Următoarele module pot fi accesate pentru a monitoriza activitatea copilului dumneavoastră pe dispozitivele mobile:

- **Poziția** - aflarea poziției curente a dispozitivului copilului dumneavoastră în Google Maps.
- **SMS** - blocarea mesajelor text de la un anumit număr de telefon.
- **Apeluri** - blocarea apelurilor de la un anumit număr de telefon.

Pentru informații suplimentare cu privire la aceste module, accesați contul dumneavoastră MyBitdefender.

21.3.1. Control web

Funcția Control web vă ajută să blocați site-urile web cu conținut neadecvat și să stabiliți restricții de timp pentru accesul la internet.

Pentru a configura funcția de Control web pentru un anumit cont de utilizator:

1. Faceți clic  pe panoul **Web** pentru a accesa fereastra **Activitate web**.
2. Utilizați selectorul pentru a activa funcția de **Control web**.

Blocarea unui site web

Pentru a bloca accesul la un site web, urmați pașii de mai jos:

1. Faceți clic pe butonul **Listă site-uri restricționate**.
2. Introduceți site-ul web în câmpul corespunzător.
3. Faceți clic pe **Adaugă**. Site-ul web va fi adăugat pe lista de site-uri blocate. Dacă vă răzgândiți, faceți clic pe butonul **Ștergere** corespunzător.

Control cuvinte cheie

Opțiunea Control cuvinte cheie vă permite să blocați accesul utilizatorilor la mesaje instant și pagini web care conțin anumite cuvinte. Folosind opțiunea Control cuvinte cheie, puteți împiedica vizualizarea de cuvinte sau expresii nepotrivite de către copiii dumneavoastră, atunci când aceștia sunt online. Mai mult, vă puteți asigura de faptul că nu se vor scurge informații cu caracter personal (precum adresa personală sau numărul de telefon) către persoane întâlnite pe internet.

Pentru a configura Controlul cuvintelor cheie pentru un anumit cont de utilizator, urmați pașii de mai jos:

1. Faceți clic pe butonul **Cuvinte cheie**.
2. Introduceți cuvântul cheie în câmpul corespunzător.
3. Faceți clic pe **Adaugă**. Dacă vă răzgândiți, faceți clic pe butonul **Ștergere** corespunzător.

Filtru de categorii

Filtrul de categorii filtrează în mod dinamic accesul la site-uri web în funcție de conținutul acestora. Atunci când setați vârsta copilului dumneavoastră, filtrul este configurat automat pentru a bloca accesul la categoriile de site-uri web considerate necorespunzătoare pentru vârsta copilului dumneavoastră. Această configurație este una potrivită pentru majoritatea situațiilor.

Dacă doriți mai mult control asupra conținutului online la care este expus copilul dumneavoastră, puteți selecta ca anumite categorii de site-uri web să fie blocate, prin intermediul Filtrului de categorii.

Pentru a configura în detaliu setările Filtrului de categorii pentru un anumit cont de utilizator, urmați pașii de mai jos:

1. Faceți clic pe butonul **Categorii**.
2. Puteți verifica care categorii web sunt blocate/restricționate în mod automat pentru grupul de vârstă selectat în prezent. Dacă setările implicite nu sunt satisfăcătoare, le puteți configura după cum doriți.
3. Faceți clic pe **Salvează**.

Restricționarea accesului la internet în funcție de oră

Puteți specifica când anume are acces copilul dumneavoastră la internet, prin intermediul opțiunilor **Program de acces la Internet** din fereastra **Activitate web**.

Pentru a configura în detaliu setările de Acces la Internet pentru un anumit cont de utilizator, urmați pașii de mai jos:

1. Faceți clic pe butonul **Programare**.
2. Selectați din grilă intervalele temporale în care accesul la internet este blocat.
3. Faceți clic pe **OK**.

21.3.2. Control aplicații

Controlul aplicațiilor vă permite să blocați rularea unei aplicații. Astfel puteți bloca jocurile, fișierele video/audio și aplicațiile de mesagerie, precum și alte categorii de aplicații, inclusiv cele periculoase.

Pentru a configura Controlul aplicațiilor pentru un anumit cont de utilizator, urmați pașii de mai jos:

1. Faceți clic  pe panoul **Aplicații** pentru a accesa fereastra **Activități aplicații**.
2. Utilizați selectorul pentru a activa funcția **Activități aplicații**.
3. Faceți clic pe butonul **Listă site-uri restricționate**.

4. Faceți clic pe **Add** pentru a adăuga aplicația în **Lista de aplicații permise** sau **Lista de aplicații restricționate**.

21.3.3. Protecție pentru Facebook

Funcția de Control parental monitorizează contul de Facebook al copilului dumneavoastră și raportează principalele activități efectuate.

Aceste activități online sunt verificate și veți primi o notificare dacă acestea se dovedesc a fi o amenințare la adresa securității contului dumneavoastră.

Printre elementele monitorizate ale contului online se numără:

- numărul de prieteni
- comentariile copilului dumneavoastră sau cele ale prietenilor săi la pozele sau link-urile publicate de acesta
- mesaje
- postări pe perete
- fotografii și filme încărcate
- setări de confidențialitate ale contului

Pentru a configura protecția pentru Facebook pentru un anumit cont de utilizator:

1. Mergeți la secțiunea **Facebook**.
2. Faceți clic pe **Conectare profil copil** în panoul **Facebook**.
3. Pentru a proteja contul de Facebook al copilului dumneavoastră, instalați aplicația corespunzătoare folosind link-ul furnizat.

21.3.4. Controlul mesageriei instant

Controlul mesageriei instant vă permite să specificați contactele cu care copilul dumneavoastră poate comunica prin chat sau să blocați accesul la mesajele instant care conțin anumite cuvinte.

Notă
Controlul mesageriei instant este disponibil doar pentru Yahoo Messenger și Windows Live (MSN) Messenger.

Pentru a configura Controlul mesageriei instant pentru un anumit cont de utilizator, urmați pașii de mai jos:

1. Mergeți la secțiunea **Mesagerie instant**.
2. Faceți clic pe panoul **Mesagerie instant** pentru a accesa fereastra **Activitate mesagerie instant**.
3. Utilizați selectorul pentru a activa funcția **Activitate mesagerie instant**.

Restricționați accesul la **Mesageria instant** folosind una dintre următoarele opțiuni disponibile:

- Buton **Listă utilizatori restricționați** pentru a introduce un nume de utilizator de mesagerie instant.
- Butonul **Cuvinte cheie** pentru a bloca accesul la mesajele instant care conțin anumite cuvinte.

22. Protecție Safego pentru rețelele sociale

Aveți încredere în prietenii dumneavoastră online, dar nu și în calculatoarele lor?Utilizați protecția Safego pentru rețelele sociale pentru a vă proteja contul și prietenii împotriva amenințărilor online.

Safego este o aplicație Bitdefender dezvoltată pentru siguranța conturilor dumneavoastră de Facebook și Twitter.Rolul său este acela de a scana link-urile pe care le primiți de la prieteni și de monitoriza setările de confidențialitate ale contului dumneavoastră.

Notă

Pentru a putea utiliza această funcție, este necesar un cont MyBitdefender. Pentru mai multe informații, consultați *„Contul MyBitdefender”* (p. 33).

Protecție Safego pentru Facebook

Acestea sunt numeroasele funcții disponibile pentru contul dumneavoastră Facebook:

- scanează automat postările din News Feed pentru link-uri periculoase.
- vă protejează contul împotriva amenințărilor online.

  În momentul în care detectează o postare sau un comentariu care este de tip spam, tentativă de phishing sau malware, veți primi un mesaj de avertizare.
- vă avertizează prietenii cu privire la link-urile suspecte postate în News Feed.
- vă ajută să vă creați o rețea sigură de prieteni cu ajutorul funcției **Friend’O’Meter**.
- efectuați o verificare a stării de securitate a sistemului cu ajutorul funcției de Scanare rapidă a Bitdefender.

Pentru a accesa Safego pentru Facebook din produsul Bitdefender, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Safego**, faceți clic pe **Administrare** și selectați **Activează pentru Facebook** din meniul derulant. Veți fi direcționat către contul dumneavoastră.

   Dacă ați activat deja Safego pentru Facebook, veți putea să accesați statisticile referitoare la activitatea sa făcând clic pe butonul **Vizualizare rapoarte pentru Facebook**.
3. Utilizați informațiile de autentificare Facebook pentru a vă conecta la aplicația Safego.
4. Permiteți opțiunii Safego să acceseze contul dumneavoastră de Facebook.

Protecție Safego pentru Twitter

Acestea sunt numeroasele funcții disponibile pentru contul dumneavoastră Twitter:

- scanează permanent contul dumneavoastră în fundal.
- când este detectată o amenințare, sunteți informat printr-un mesaj direct pentru a putea lua măsurile necesare și a-l neutraliza.
- trimite un mesaj direct din contul dumneavoastră către persoanele din lista dumneavoastră de Urmărire în ale căror conturi s-au detectat probleme.
- scanează mesajele dumneavoastră private pentru identificarea elementelor de spam, phishing și a programelor periculoase.
- postează automat statistici de securitate cu privire la activitatea din contul dumneavoastră.

Pentru a accesa Safego pentru Twitter din produsul Bitdefender, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. În panoul **Safego**, faceți clic pe **Administrare** și selectați **Activează pentru Twitter** din meniul derulant. Veți fi direcționat către contul dumneavoastră.

   Dacă ați activat deja Safego pentru Twitter, veți putea să accesați statisticile referitoare la activitatea sa făcând clic pe butonul **Vizualizare rapoarte pentru Twitter**.
3. Utilizați informațiile de autentificare Twitter pentru a vă conecta la aplicația Safego.
4. Permiteți opțiunii Safego să acceseze contul dumneavoastră de Twitter.

23. Bitdefender USB Immunizer

Funcția Autorun încorporată în sistemele de operare Windows este un instrument foarte util care permite calculatoarelor să execute automat un fișier de pe un suport conectat la acestea. De exemplu, instalările aplicațiilor pot începe automat când introduceți un CD în unitatea optică.

Din nefericire, această funcție poate fi utilizată și de programele periculoase pentru lansarea automată și infiltrarea în calculatorul dumneavoastră de pe medii reinscriptibile, cum ar fi unitățile USB și cardurile de memorie conectate prin cititoare de carduri. În ultimii ani au fost create numeroase atacuri bazate pe Autorun.

Cu USB Immunizer, puteți împiedica orice unități flash formatate NTFS, FAT32 sau FAT să mai execute programe periculoase. După ce un dispozitiv USB a fost imunizat, programele periculoase nu îl mai pot configura să ruleze o anumită aplicație când dispozitivul este conectat la un calculator pe care rulează Windows.

Pentru imunizarea unui dispozitiv USB, urmați pașii de mai jos:

1. Conectați unitatea flash la calculatorul dumneavoastră.
2. Navigați în calculator pentru a localiza dispozitivul amovibl de stocare și faceți clic dreapta pe această pictogramă.
3. În meniul contextual, evidențiați **Bitdefender** și selectați **Imunizează această unitate**.

Notă

Dacă dispozitivul a fost deja imunizat, în locul opțiunii Imunizare va apărea mesajul **Dispozitivul USB este protejat împotriva programelor periculoase cu executare automată**

Pentru a preveni lansarea programelor periculoase de către calculatorul dumneavoastră de pe dispozitive USB neimunizate, dezactivați funcția de rulare automată a mediilor. Pentru mai multe informații, consultați *„Cu ajutorul monitorizării automate a vulnerabilităților”* (p. 86).

24. Gestionarea de la distanță a calculatoarelor dumneavoastră

Contul MyBitdefender vă permite să gestionați de la distanță produsele Bitdefender instalate pe calculatorul dumneavoastră.

Folosiți MyBitdefender pentru a crea și pune în aplicare diverse sarcini pe calculatoarele dumneavoastră de oriunde.

Un calculator va fi gestionat din contul MyBitdefender dacă îndeplinește următoarele condiții:

- aveți instalat pe calculator un produs Bitdefender 2013
- ați asociat produsul Bitdefender la contul MyBitdefender.
- calculatorul este conectat la Internet

24.1. Accesarea MyBitdefender

Bitdefender vă permite să controlați securitatea calculatoarelor dumneavoastră prin adăugarea de sarcini la produsele Bitdefender.

Prin intermediul Bitdefender vă puteți accesa contul MyBitdefender de la orice calculator sau dispozitiv mobil conectat la Internet.

Accesați MyBitdefender:

- Pe orice dispozitiv cu acces la Internet:
  1. Deschideți un browser web.
  2. Mergeți la:https://my.bitdefender.com
  3. Conectați-vă la contul dumneavoastră cu ajutorul numelui de utilizator și parolei.
- Din interfața Bitdefender 2013:
  1. Deschideți fereastra Bitdefender.
  2. Faceți clic pe butonul **MyBitdefender** din partea de sus a ferestrei și selectați **Panou de control** din meniul derulant.

24.2. Rularea sarcinilor pe computere

Pentru a rula o sarcină pe unul dintre calculatoare, accesați-vă contul MyBitdefender.

Dacă faceți clic pe pictograma unui calculator din partea de jos a ferestrei, puteți vedea toate sarcinile administrative pe care le puteți rula de la distanță pe calculatorul respectiv.

Înregistrare produs
: Vă permite să înregistrați Bitdefender pe un calculator de la distanță, prin introducerea unei serii de înregistrare.

Scanare completă a sistemului
Vă permite să efectuați o scanare completă pe calculatorul de la distanță.

Scanarea zonelor critice ale sistemului pentru a detecta aplicațiile periculoase
Vă permite să efectuați o scanare rapidă pe calculatorul de la distanță.

Remedierea problemelor critice
Vă permite să remediați problemele care afectează securitatea calculatorului de la distanță.

Actualizare produs
Inițiază procesul de actualizare a produsului Bitdefender instalat pe acest calculator.

Remedierea problemelor

25. Soluționarea problemelor frecvente

Acest capitol prezintă anumite probleme cu care vă puteți confrunta la utilizarea Bitdefender și vă oferă soluții posibile la aceste probleme.Majoritatea acestor probleme pot fi soluționate prin configurarea adecvată a setărilor produsului.

- *„Sistemul meu funcționează lent”* (p. 131)
- *„Nu începe scanarea”* (p. 132)
- *„Nu mai pot utiliza o anumită aplicație”* (p. 133)
- *„Nu mă pot conecta la internet”* (p. 134)
- *„Nu pot accesa un dispozitiv din rețeaua mea”* (p. 134)
- *„Conexiunea mea la internet este lentă”* (p. 136)
- *„Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet”* (p. 137)
- *„Calculatorul meu nu este conectat la Internet. Cum actualizez Bitdefender?”* (p. 137)
- *„Serviciile Bitdefender nu răspund”* (p. 138)
- *„Filtrul Antispam nu funcționează corespunzător”* (p. 139)
- *„Nu s-a reușit dezinstalarea Bitdefender”* (p. 143)
- *„Sistemul meu nu pornește după ce am instalat Bitdefender”* (p. 144)

Dacă problema dumneavoastră nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic a Bitdefender folosind informațiile din capitolul *„Solicitarea ajutorului”* (p. 156).

25.1. Sistemul meu funcționează lent

De obicei, după instalarea unui program de securitate, este posibil să se producă o ușoară încetinire a funcționării sistemului, fapt ce este normal într-o anumită măsură.

În cazul în care observați o încetinire semnificativă, această problemă poate apărea din următoarele motive:

- **Bitdefender nu este singurul program de securitate instalat în sistem.**

  Deși Bitdefender caută și dezinstalează programele de securitate detectate în timpul instalării, se recomandă să îndepărtați orice alte programe antivirus pe care le-ați utilizat înainte de a iniția instalarea Bitdefender.Pentru mai multe informații, consultați *„Cum dezinstalez alte soluții de securitate?”* (p. 58).

- **Nu sunt îndeplinite cerințele minime de sistem pentru rularea Bitdefender.**

În cazul în care computerul dumneavoastră nu îndeplinește cerințele minime de sistem, acesta va începe să răspundă lent, mai ales atunci când mai multe aplicații rulează în același timp.Pentru mai multe informații, consultați *„Cerințe minime de sistem”* (p. 3).

- **Unitățile de hard disc sunt prea fragmentate.**

  Fragmentarea fișierelor încetinește accesul la acestea și scade performanțele sistemului.

  Pentru a vă defragmenta partițiile de disc folosind instrumentul din Windows, urmați calea din meniul Start al Windows: **Start → All Programs → Accessories → System Tools → Disk Defragmenter**.

25.2. Nu începe scanarea

Acest tip de problemă poate avea două cauze principale:

- **O instalare anterioară a Bitdefender care nu a fost complet eliminată sau o instalare necorespunzătoare a Bitdefender**.

  În acest caz, urmați acești pași:

  1. Dezinstalați complet Bitdefender din sistem:
     a. Mergeți la http://www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.
     b. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.
     c. Reporniți calculatorul.
  2. Reinstalați Bitdefender în sistem.

- **Bitdefender nu este singura soluție de securitate instalată în sistemul dumneavoastră**.

  În acest caz, urmați acești pași:

  1. Dezinstalați cealaltă soluție de securitate. Pentru mai multe informații, consultați *„Cum dezinstalez alte soluții de securitate?”* (p. 58).
  2. Dezinstalați complet Bitdefender din sistem:
     a. Mergeți la http://www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.
     b. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.
     c. Reporniți calculatorul.
  3. Reinstalați Bitdefender în sistem.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 156).

25.3. Nu mai pot utiliza o anumită aplicație

Această problemă apare când încercați să utilizați un program care a funcționat normal înainte de instalarea Bitdefender.

Vă puteți confrunta cu una dintre următoarele situații:

- Este posibil să primiți un mesaj din partea Bitdefender referitor la faptul că programul încearcă să efectueze o modificare asupra sistemului.
- Este posibil să primiți un mesaj de eroare din partea programului pe care încercați să-l utilizați.

Acest tip de situație apare când Active Virus Control detectează din greșeală anumite aplicații ca fiind rău intenționate.

Active Virus Control este un modul Bitdefender care monitorizează în mod constant aplicațiile care rulează pe sistemul dumneavoastră și raportează acele aplicații care sunt posibil rău intenționate. Deoarece această opțiune se bazează pe un sistem euristic, pot exista situații în care aplicații legitime să fie raportate de Active Virus Control.

Atunci când se întâmplă aceasta, puteți exclude aplicația respectivă de la monitorizarea efectuată de Active Virus Control.

Pentru a adăuga programul în lista de excluderi, urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară..
3. În fereastra **Prezentare setări**, selectați **Antivirus**.
4. În fereastra **Setări antivirus**, selectați secțiunea **Excluderi**.
5. Faceți clic pe link-ul **Procese excluse**. În fereastra care va apărea, puteți gestiona excepțiile de la procesul Active Virus Control.
6. Pentru a adăuga excepții, urmați pașii de mai jos:
   a. Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
   b. Faceți clic pe **Caută**, identificați și selectați aplicația care doriți să fie exclusă și faceți clic pe **OK**.
   c. Mențineți selectată opțiunea **Permite** pentru a preveni blocarea aplicației de către Active Virus Control.
   d. Faceți clic pe **Adaugă**.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 156).

25.4. Nu mă pot conecta la internet

Este posibil să observați că un program sau un browser de internet nu se mai poate conecta la internet sau accesa serviciile de rețea după instalarea Bitdefender.

În acest caz, cea mai bună soluție este să configurați Bitdefender să permită în mod automat conexiunile către și de la aplicația software respectivă.

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară..
3. În fereastra **Prezentare setări**, selectați **Firewall**.
4. În fereastra **Setări firewall**, selectați secțiunea **Setări**.
5. Sub Reguli Firewall faceți clic pe **Reguli aplicație**.
6. Pentru a adăuga o regulă privind aplicația, faceți clic pe butonul corespunzător.
7. Faceți clic pe **Caută** și selectați aplicația căreia i se aplică regula.
8. Selectați tipurile de rețea disponibile.
9. Mergeți la **Permisiune** și selectați **Permite**.

Închideți Bitdefender, deschideți aplicația software și încercați din nou să vă conectați la internet.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 156).

25.5. Nu pot accesa un dispozitiv din rețeaua mea

În funcție de rețeaua la care sunteți conectat, firewallul Bitdefender poate bloca conexiunea dintre sistemul dumneavoastră și un alt dispozitiv (cum ar fi un alt computer sau o imprimantă). În consecință, nu mai puteți partaja sau imprima fișiere.

În acest caz, cea mai bună soluție este să configurați Bitdefender să permită în mod automat conexiunile către și de la dispozitivul respectiv. Pentru fiecare conexiune din rețea, puteți configura o zonă specială securizată.

O zonă de încredere este un dispozitiv în care aveți deplină încredere. Este permis necondiționat traficul dintre computerul dumneavoastră și un dispozitiv de încredere. Pentru a partaja resursele cu anumite dispozitive, precum computere sau imprimante, adăugați aceste dispozitive ca fiind de încredere.

Pentru a adăuga o zonă de încredere pe adaptorii rețelei dumneavoastră, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară..

3. În fereastra **Prezentare setări**, selectați **Firewall**.
4. În fereastra **Setări firewall**, selectați secțiunea **Setări**.
5. Sub Reguli Firewall faceți clic pe **Reguli adaptor**.
6. Pentru a adăuga o secțiune, faceți clic pe butonul corespunzător. Va apărea o nouă fereastră în care vor fi afișate adresele IP ale dispozitivelor conectate la rețea.
7. Selectați adresa de IP a computerului sau a imprimantei pe care doriți să o adăugați sau introduceți un interval de adrese în căsuța corespunzătoare.
8. Mergeți la **Permisiune** și selectați **Permite**.

Dacă tot nu vă puteți conecta la dispozitiv, este posibil ca problema să nu fie cauzată de Bitdefender.

Verificați alte cauze posibile, cum ar fi:

- Firewallul de pe celălalt calculator poate bloca partajarea de fișiere și imprimante cu calculatorul dumneavoastră.
  - Dacă se folosește Windows Firewall, acesta poate fi configurat să permită partajarea de fișiere și imprimante, după cum urmează: deschideți fereastra de setări a Windows Firewall, tabul **Exceptions**, și selectați căsuța **File and Printer Sharing**.
  - Dacă se folosește un alt program firewall, consultați documentația sau fișierul de ajutor ale acestuia.
- Cauze generale care pot împiedica folosirea sau conectarea la imprimanta partajată:
  - Poate fi necesar să vă conectați la un cont Windows de administrator pentru a avea acces la imprimanta partajată.
  - Numai anumite calculatoare și anumiți utilizatori pot accesa imprimanta partajată. Dacă partajați imprimanta dumneavoastră, verificați restricțiile de acces stabilite pentru aceasta pentru a vedea dacă utilizatorul de pe celălalt calculator o poate accesa. Dacă încercați să vă conectați la o imprimantă partajată, întrebați utilizatorul de pe celălalt calculator dacă vi se permite accesul la imprimantă.
  - Imprimanta conectată la calculatorul dumneavoastră sau la celălalt calculator nu este partajată.
  - Imprimanta partajată nu este adăugată pe calculator.

Notă

Pentru a afla cum să administrați imprimantele partajate (partajarea unei imprimante, stabilirea sau eliminarea permisiunilor de acces la o imprimantă,

conectarea la o imprimantă de rețea sau partajată), mergeți la Centrul de Asistență și Suport al Windows (în meniul Start, faceți clic pe **Help and Support**).

- Accesul la o imprimantă din rețea poate fi restricționat pentru anumite computere sau pentru anumiți utilizatori. Este recomandat să consultați administratorul rețelei pentru a afla dacă vă puteți conecta la imprimanta în cauză.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 156).

25.6. Conexiunea mea la internet este lentă

Această situație poate apărea după instalarea Bitdefender. Problema poate fi cauzată de erori de configurare a firewallului Bitdefender.

Pentru a remedia această situație, urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Din panoul **Firewall**, faceți clic pe buton pentru a dezactiva **Firewall-ul**.
3. Verificați dacă, după ce ați dezactivat firewallul Bitdefender, conexiunea dumneavoastră la internet s-a îmbunătățit.
   - Dacă nu se remediază problema cu viteza redusă a conexiunii la Internet, este posibil ca problema să nu fie cauzată de Bitdefender. Trebuie să contactați furnizorul dumneavoastră de servicii de internet pentru a verifica dacă conexiunea este funcțională la nivelul acestuia.

     În cazul în care primiți o confirmare din partea furnizorului dumneavoastră de servicii de internet că respectiva conexiune este funcțională la nivelul său, iar problema încă persistă, contactați Bitdefender conform descrierii din secțiunea *„Solicitarea ajutorului”* (p. 156).
   - În cazul în care conexiunea la internet s-a îmbunătățit după dezactivarea firewallului Bitdefender, urmați acești pași:
     a. Deschideți fereastra Bitdefender.
     b. Din panoul **Firewall**, faceți clic pe buton pentru a activa **Firewall-ul**.
     c. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară..
     d. În fereastra **Prezentare setări**, selectați **Firewall**.
     e. În fereastra **Setări firewall**, selectați secțiunea **Avansat**.
     f. Mergeți la **Partajare conexiune la internet** și faceți clic pe comutator pentru activare.
     g. Mergeți la **Blocare scanare porturi** și faceți clic pe comutator pentru dezactivare.

h. Faceți clic pe  pentru a reveni la fereastra principală.

i. În panoul **Firewall**, faceți clic pe **Administrare adaptoare**.

j. Accesați **Tip de rețea** și selectați **Acasă/Birou**.

k. Accesați **Modul ascuns** și setați-l la **La distanță**. Setați **Generic** la **Da**.

l. Închideți Bitdefender, reporniți sistemul ș verificați viteza conexiunii la internet.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 156).

25.7. Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet

Dacă dispuneți de o conexiune lentă la internet (cum ar fi cea de tip dial-up), în timpul procesului de actualizare pot apărea erori.

Pentru a vă menține actualizat sistemul cu cele mai recente semnături malware Bitdefender, urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentare setări**, selectați **Actualizare**.
4. În fereastra **Setări actualizare**, selectați secțiunea **Actualizare**.
5. Sub opțiunea **Actualizare reguli de procesare**, selectați **Anunță înainte de descărcare**.
6. Faceți clic pe  pentru a reveni la fereastra principală.
7. Mergeți la panoul **Actualizare** și faceți clic pe **Actualizează acum**.
8. Selectați numai **Actualizări semnături** și apoi faceți clic pe **OK**.
9. Bitdefender va descărca și va instala numai actualizările semnăturilor malware.

25.8. Calculatorul meu nu este conectat la Internet. Cum actualizez Bitdefender?

În cazul în care calculatorul dumneavoastră nu este conectat la internet, trebuie să descărcați manual actualizările pe un calculator cu acces la internet și apoi să le transferați pe calculatorul dumneavoastră utilizând un dispozitiv de stocare portabil, cum ar fi un stick USB.

Urmați acești pași:

1. Pe un calculator cu acces la internet, deschideți un browser și accesați:

   http://www.bitdefender.ro/site/view/Desktop-Products-Updates.html

2. În coloana **Actualizare manuală**, faceți clic pe linkul corespunzător produsului și arhitecturii sistemului dumneavoastră. În cazul în care nu știți dacă sistemul dumneavoastră Windows rulează pe 32 sau 64 de biți, consultați *„Utilizez o versiune Windows pe 32 biți sau pe 64 biți?”* (p. 57).

3. Salvați fișierul denumit `weekly.exe` în sistem.

4. Transferați fișierul descărcat pe un dispozitiv de stocare portabil, cum ar fi un stick USB, și apoi în calculatorul dumneavoastră.

5. Faceți dublu-clic pe fișier și urmați indicațiile programului asistent.

25.9. Serviciile Bitdefender nu răspund

Acest articol vă ajută să remediați problema **Serviciile Bitdefender nu răspund**. Această problemă poate apărea în următoarele situații:

- Pictograma Bitdefender din bara de sistem este afișată în culoarea gri și veți fi notificat de faptul să serviciile Bitdefender nu răspund.
- Fereastra Bitdefender indică faptul că serviciile Bitdefender nu răspund.

Problema poate fi cauzată de:

- o actualizare importantă este în curs de instalare.
- erori temporare de comunicare între serviciile Bitdefender.
- unele dintre serviciile Bitdefender sunt oprite.
- alte soluții de securitate rulează pe calculatorul dumneavoastră, în același timp cu Bitdefender.

Pentru a remedia această problemă, încercați următoarele soluții:

1. Așteptați câteva momente pentru a vedea dacă apar schimbări. Eroarea poate fi temporară.

2. Reporniți calculatorul și așteptați câteva momente până când se încarcă Bitdefender. Deschideți Bitdefender pentru a vedea dacă eroarea persistă. De obicei, repornirea calculatorului rezolvă problema.

3. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați Bitdefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați Bitdefender.

   Pentru mai multe informații, consultați *„Cum dezinstalez alte soluții de securitate?”* (p. 58).

Dacă eroarea persistă, vă rugăm să contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea *„Solicitarea ajutorului”* (p. 156).

25.10. Filtrul Antispam nu funcționează corespunzător

Acest articol vă ajută să remediați următoarele probleme legate de funcționarea filtrului antispam al Bitdefender:

- Mai multe mesaje e-mail legitime sunt marcate ca [spam].
- Multe mesaje spam nu sunt marcate corespunzător de filtrul antispam.
- Filtrul antispam nu detectează niciun mesaj spam.

25.10.1. Mesaje legitime sunt marcate ca [spam]

Mesaje legitime sunt marcate ca [spam] pentru că filtrul antispam Bitdefender le percepe ca atare. În mod normal, puteți rezolva această problemă printr-o configurare adecvată a filtrului Antispam.

Bitdefender adaugă automat într-o Listă de prieteni destinatarii mesajelor e-mail trimise de dumneavoastră. Mesajele e-mail primite de la persoanele de pe Lista de prieteni sunt considerate a fi legitime. Ele nu sunt verificate de filtrul antispam și, astfel, nu sunt marcate niciodată ca [spam].

Configurarea automată a Listei de prieteni nu previne erorile de detecție care pot apărea în următoarele situații:

- Primiți multe mesaje comerciale nesolicitate, ca urmare a înscrierii pe diferite site-uri web. În acest caz, soluția este să adăugați adresele de e-mail de la care primiți astfel de mesaje în Lista de prieteni.
- O parte semnificativă a mesajelor e-mail pe care le primiți sunt trimise de oameni cărora nu le-ați scris niciodată pe e-mail, cum ar fi: clienți, potențiali parteneri de afaceri și alții. În acest caz, sunt necesare alte soluții.

  1. Dacă folosiți unul dintre clienții de e-mail în care se integrează Bitdefender, indicați erorile de detecție.

     Notă
     Bitdefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de mail admiși, consultați *„Clienți și protocoale de e-mail compatibile”* (p. 91).

  2. Scăderea nivelului de protecție antispam. Prin scăderea nivelului de protecție antispam, filtrul antispam va avea nevoie de mai multe indicii pentru a clasifica un mesaj e-mail ca spam. Încercați această soluție numai dacă multe mesaje legitime (inclusiv mesaje comerciale solicitate) sunt incorect detectate ca spam.

Adăugați-vă contactele pe Lista de prieteni

Dacă folosiți un client de mail admis, puteți adăuga foarte ușor expeditorii de mesaje legitime pe Lista de prieteni. Urmați acești pași:

1. În clientul dumneavoastră de mail, selectați un mesaj e-mail al expeditorului pe care doriți să-l adăugați pe Lista de prieteni.
2. Faceți clic pe butonul **Adaugă prieten** din bara de instrumente antispam Bitdefender.
3. Vi se poate cere să confirmați adresa adăugată pe Lista de prieteni. Selectați **Nu mai afișa acest mesaj** și faceți clic pe **OK**.

Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.

Dacă folosiți un alt client de mail, puteți adăuga contacte pe Lista de prieteni din interfața Bitdefender. Urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antispam**, faceți clic pe **Administrare** și selectați **Prieteni** din meniul derulant.

   Va apărea o fereastră de configurare.
3. Introduceți adresa de e-mail de la care doriți să primiți mereu mesaje și apoi faceți clic pe **Adăugare**.Puteți adăuga oricâte adrese de e-mail doriți.
4. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Indicați erorile de detecție

Dacă folosiți un client de e-mail compatibil, puteți corecta cu ușurință filtrul antispam (indicând ce mesaje e-mail nu ar fi trebuit marcate ca fiind de tip `[spam]`). Astfel, veți îmbunătăți eficiența filtrului antispam.Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele legitime pe care Bitdefender le-a marcat incorect ca `[spam]`.
4. Faceți clic pe butonul **Adaugă prieten** din bara de instrumente antispam Bitdefender, pentru a adăuga expeditorul pe Lista de prieteni.Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare.Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.
5. Faceți clic pe butonul **Nu este spam** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail).Mesajul e-mail va fi mutat în directorul Mesaje primite.

Reduceți nivelul de protecție antispam

Pentru a reduce nivelul protecției antispam, urmați acești pași:

1. Deschideți fereastra Bitdefender.

2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentarea setărilor**, selectați **Antispam**.
4. În fereastra **Setări Antispam**, selectați secțiunea **Setări**.
5. Mutați cursorul mai jos pe scală.

25.10.2. Numeroase mesaje spam nu sunt detectate

Dacă primiți multe mesaje spam care nu sunt marcate [spam], trebuie să configurați filtrul antispam Bitdefender, pentru a-i îmbunătăți eficiența.

Încercați următoarele soluții:

1. Dacă folosiți unul dintre clienții de e-mail în care se integrează Bitdefender, indicați mesajele spam nedetectate.

   Notă

   Bitdefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat.Pentru o listă completă a clienților de mail admiși, consultați *„Clienți și protocoale de e-mail compatibile”* (p. 91).

2. Adăugați spammerii pe Lista de spammeri. Mesajele e-mail primite de la adrese de pe Lista de spammeri sunt marcate automat ca [spam].
3. Creșteți nivelul protecției antispam. Prin creșterea nivelului de protecție antispam, filtrul antispam va avea nevoie de mai puține indicii pentru a clasifica un mesaj e-mail ca spam.

Indicați mesajele spam nedetectate

Dacă folosiți un client de mail admis, puteți indica cu ușurință care mesaje e-mail ar fi trebuit detectate ca spam. Astfel, veți îmbunătăți eficiența filtrului antispam.Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți la directorul Inbox.
3. Selectați mesajele spam nedetectate.
4. Faceți clic pe butonul **Spam** din bara de instrumente antispam Bitdefender (localizată, în mod normal, în partea superioară a ferestrei clientului de e-mail). Acestea sunt marcate imediat ca [spam] și mutate în directorul de mesaje nesolicitate (junk).

Adăugați spammeri pe Lista de spammeri

Dacă folosiți un client de mail admis, puteți adăuga foarte ușor expeditorii de mesaje spam pe Lista de spammeri.Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele pe care Bitdefender le-a marcat ca `[spam]`.
4. Faceți clic pe butonul **Adaugă spammer** din bara de instrumente antispam Bitdefender.
5. Vi se poate cere să confirmați adresa adăugată pe Lista de spammeri.Selectați **Nu mai afișa acest mesaj** și faceți clic pe **OK**.

Dacă folosiți un alt client de mail, puteți adăuga manual spammeri în Lista de spammeri din interfața Bitdefender. Este recomandat să procedați astfel numai atunci când ați primit mai multe mesaje spam de la aceeași adresă de e-mail.Urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. În panoul **Antispam**, faceți clic pe **Administrare** și selectați **Spammeri** din meniul derulant.

   Va apărea o fereastră de configurare.
3. Introduceți adresa de e-mail a spammer-ului și apoi faceți clic pe **Adăugare**.Puteți adăuga oricâte adrese de e-mail doriți.
4. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Sporiți nivelul protecției antispam

Pentru a crește nivelul protecției antispam, urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe butonul **Setări** de pe bara de instrumente din parte superioară.
3. În fereastra **Prezentarea setărilor**, selectați **Antispam**.
4. În fereastra **Setări Antispam**, selectați secțiunea **Setări**.
5. Mutați cursorul mai sus pe scală.

25.10.3. Filtrul antispam nu detectează niciun mesaj spam

Dacă niciun mesaj spam nu este marcat ca `[spam]`, este posibil să existe probleme legate de filtrul Antispam Bitdefender.Înainte de a remedia această problemă, asigurați-vă că ea nu se datorează următoarelor cauze:

- Este posibil ca protecția antispam să fie dezactivată.Pentru a verifica starea protecției antispam, deschideți fereastra Bitdefender și verificați selectorul din panoul **Antispam**.

Dacă protecția Antispam este dezactivată, aceasta este cauza problemei dvs.Faceți clic pe selector pentru a activa protecția anstispam.

- Protecția antispam Bitdefender este disponibilă numai pentru clienții de e-mail configurați să primească mesaje e-mail prin protocolul POP3.Aceasta înseamnă că:
  - Mesajele e-mail primite prin servicii de e-mail oferite online (cum ar fi Yahoo, Gmail, Hotmail sau altele) nu sunt supuse verificării antispam de către Bitdefender.
  - Dacă aveți un client de e-mail configurat să primească mesaje prin alt protocol decât POP3 (de exemplu IMAP4), Bitdefender nu supune aceste mesaje unei verificări antispam.

  Notă

  POP3 este unul dintre cele mai des folosite protocoale de descărcare a mesajelor e-mail de pe un server de mail.Dacă nu știți ce protocol folosește clientul dumneavoastră de e-mail pentru a descărca mesajele, întrebați persoana care l-a configurat.

- Bitdefender Internet Security 2013 nu scanează traficul POP3 generat de Lotus Notes.

O soluție posibilă este repararea sau reinstalarea produsului. Dacă doriți, puteți contacta Bitdefender pentru suport, folosind informațiile din secțiunea *„Solicitarea ajutorului”* (p. 156).

25.11. Nu s-a reușit dezinstalarea Bitdefender

Acest articol vă ajută să remediați erorile care pot apărea la dezinstalarea Bitdefender. Sunt posibile două situații:

- În timpul dezinstalării apare un ecran de eroare. Ecranul oferă un buton pentru rularea unui instrument de dezinstalare, care va curăța sistemul.
- Dezinstalarea nu înaintează și, eventual, sistemul se blochează. Faceți clic pe **Anulare** pentru a abandona dezinstalarea. Dacă anularea nu este posibilă, reporniți sistemul.

Dacă dezinstalarea eșuează, unele chei de regiștri și fișiere Bitdefender pot rămâne în sistemul dvs. Aceste rămășite pot împiedica instalarea ulterioară a Bitdefender. De asemenea, ele pot afecta funcționarea și stabilitatea sistemului.

Pentru a șterge definitiv Bitdefender de pe sistemul dumneavoastră, urmați pașii de mai jos:

1. Mergeți la http://www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.

2. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.
3. Reporniți calculatorul.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 156).

25.12. Sistemul meu nu pornește după ce am instalat Bitdefender

Dacă se întâmplă ca, după ce tocmai ați instalat Bitdefender,să nu puteți reporni sistemul în modul normal, pot exista mai multe motive pentru această problemă.

Cel mai probabil această problemă este cauzată fie de o instalare anterioară a Bitdefender care nu a fost dezinstalată corespunzător fie de o altă soluție de securitate care este instalată pe sistem.

Mai jos sunt prezentate modurile în care să acționați pentru fiecare situație:

- **Ați avut Bitdefender instalat anterior și acesta nu a fost dezinstalat corespunzător.**

  Pentru a soluționa această problemă, urmați pașii de mai jos:

  1. Reporniți sistemul în Safe Mode. Pentru a afla cum să procedați, consultați *„Cum pot să repornesc sistemul în Safe Mode?”* (p. 60).
  2. Ștergeți Bitdefender din sistemul dumneavoastră:
     a. Mergeți la http://www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.
     b. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.
     c. Reporniți calculatorul.
  3. Reporniți sistemul în modul normal și reinstalați Bitdefender.

- **Ați avut instalată o altă soluție de securitate înainte, iar aceasta nu a fost dezinstalată corespunzător.**

  Pentru a soluționa această problemă, urmați pașii de mai jos:

  1. Reporniți sistemul în Safe Mode. Pentru a afla cum să procedați, consultați *„Cum pot să repornesc sistemul în Safe Mode?”* (p. 60).
  2. Ștergeți Bitdefender din sistemul dumneavoastră:
     a. Mergeți la http://www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.
     b. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.

c. Reporniți calculatorul.

3. Pentru a dezinstala celălalt software în mod corect, mergeți pe site-ul web al producătorului și lansați instrumentul de dezinstalare sau contactați direct producătorul, solicitând instrucțiunile de dezinstalare.
4. Reporniți sistemul în modul normal și reinstalați Bitdefender.

Situația nu s-a rezolvat deși ați urmat toți pașii de mai sus.

Pentru a soluționa această problemă, urmați pașii de mai jos:

1. Reporniți sistemul în Safe Mode. Pentru a afla cum să procedați, consultați *„Cum pot să repornesc sistemul în Safe Mode?”* (p. 60).
2. Cu ajutorul funcției System Restore din Windows puteți restabili computerul la o dată anterioară instalării produsului Bitdefender. Pentru a afla cum să procedați, consultați *„Cum folosesc funcția System Restore în Windows?”* (p. 59).
3. Reporniți sistemul în modul normal și contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea *„Solicitarea ajutorului”* (p. 156).

26. Eliminarea programelor malware din sistemul dumneavoastră

Virușii și celelalte amenințări malware vă pot afecta sistemul în moduri diferite, iar modul de acțiune al Bitdefender depinde de tipul de atac malware.Deoarece virușii își schimbă comportamentul în mod frecvent, este dificil de stabilit un model privind comportamentul și acțiunile acestora.

Există cazuri când Bitdefender nu poate elimina în mod automat infecția malware din sistemul dumneavoastră.În astfel de cazuri, este necesară intervenția dumneavoastră.

- *„Modul de salvare Bitdefender”* (p. 146)
- *„Ce trebuie să faceți atunci când Bitdefender detectează viruși pe computerul dumneavoastră?”* (p. 148)
- *„Cum elimin un virus dintr-o arhivă?”* (p. 149)
- *„Cum elimin un virus dintr-o arhivă de e-mail?”* (p. 150)
- *„Ce trebuie să fac dacă suspectez că un fișier este periculos?”* (p. 151)
- *„Cum să curățați fișierele infectate din System Volume Information”* (p. 151)
- *„Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare?”* (p. 153)
- *„Ce reprezintă elementele omise din jurnalul de scanare?”* (p. 153)
- *„Ce reprezintă fișierele supracomprimate din jurnalul de scanare?”* (p. 153)
- *„De ce Bitdefender a șters în mod automat un fișier infectat?”* (p. 154)

Dacă problema dumneavoastră nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic a Bitdefender folosind informațiile din capitolul *„Solicitarea ajutorului”* (p. 156).

26.1. Modul de salvare Bitdefender

Modul de salvare este o caracteristică a Bitdefender care vă permite să scanați și să dezinfectați toate partițiile hard discului de pe sistemul de operare.

După ce ați instalat Bitdefender Internet Security 2013, Modul de salvare poate fi utilizat chiar dacă nu mai puteți reporni sistemul din Windows.

Pornirea sistemului în Modul de salvare

Puteți accesa Modul de salvare în unul dintre următoarele două moduri:

Din fereastra Bitdefender

Pentru a accesa Modul de salvare direct din Bitdefender, urmați acești pași:

1. Deschideți fereastra Bitdefender.

2. În panoul **Antivirus**, faceți clic pe **Scanează acum** și selectați **Mod de salvare** din meniul derulant.

   Va apărea o fereastră de configurare. Faceți clic pe **Da** pentru a reporni calculatorul.

3. După ce este repornit computerul, va apărea un meniu care vă va solicita să selectați un sistem de operare. Alegeți **imaginea de salvare Bitdefender** și apăsați pe tasta **Enter** pentru a reporni dintr-un mediu Bitdefender de unde vă puteți curăța partiția Windows.

4. În cazul în care vi se solicită, apăsați **Enter** și ajustați rezoluția ecranului la valoarea cea mai apropiată de cea pe care o folosiți de obicei. Apoi apăsați din nou pe **Enter**.

   Modul de salvare pentru Bitdefender se va încărca în câteva momente.

Porniți computerul direct în Modul de salvare

În cazul în care nu mai pornește Windows, puteți porni computerul direct în Modul de salvare al Bitdefender, urmând pașii de mai jos.

Notă

Această metodă nu este disponibilă pe computerele pe care rulează Windows XP.

1. Porniți / reporniți computerul și începeți să apăsați pe tasta **space** de pe tastatură înainte de apariția logoului Windows.

2. Va fi afișat un meniu care vă va ruga să selectați un sistem de operare pentru a începe. Apăsați pe **TAB** pentru a accesa zona instrumentelor. Alegeți **imaginea de salvare Bitdefender** și apăsați pe tasta **Enter** pentru a reporni dintr-un mediu Bitdefender de unde vă puteți curăța partiția Windows.

3. În cazul în care vi se solicită, apăsați **Enter** și ajustați rezoluția ecranului la valoarea cea mai apropiată de cea pe care o folosiți de obicei. Apoi apăsați din nou pe **Enter**.

   Modul de salvare pentru Bitdefender se va încărca în câteva momente.

Scanarea sistemului în Modul de salvare

Pentru a scana sistemul atunci când se află în Modul de salvare, urmați pașii de mai jos:

1. Accesați modul de salvare, conform descrierii din „Pornirea sistemului în Modul de salvare” (p. 146).
2. Va apărea logo-ul Bitdefender și motoarele antivirus vor începe să fie copiate.
3. Va fi afișată o fereastră de întâmpinare. Faceți clic pe **Continue**.
4. Este inițiată o actualizare a semnăturilor antivirus.

5. După ce s-a finalizat actualizarea, va apărea fereastra pentru scanarea antivirus la cerere a Bitdefender.
6. Faceți clic pe **Scanează acum**, selectați ținta de scanat din fereastra care apare și faceți clic pe **Deschidere** pentru a începe scanarea.

   Este recomandat scanarea întregii partiții Windows.

   Notă

   Atunci când lucrați în Modul de salvare, veți întâlni denumiri de partiții de tip Linux. Partițiile discului vor fi afișate ca `sda1` corespunzând probabil `(C:)` partiție de tip Windows, `sda2` corespunzând `(D:)` și așa mai departe..

7. Așteptați finalizarea procesului de scanare. Dacă este detectat vreun program malware, urmați instrucțiunile pentru a elimina amenințarea.
8. Pentru a ieși din Modul de salvare, faceți clic dreapta în secțiunea liberă de pe desktop, selectați **Deconectare** din meniul care apare și apoi selectați dacă doriți să reporniți sau să închideți computerul.

26.2. Ce trebuie să faceți atunci când Bitdefender detectează viruși pe computerul dumneavoastră?

Puteți afla că în calculatorul dumneavoastră se află un virus într-unul dintre aceste moduri:

- V-ați scanat calculatorul și Bitdefender a găsit elemente infectate pe acesta.
- O alertă de viruși vă informează că Bitdefender a blocat unul sau mai mulți viruși pe calculatorul dumneavoastră.

În astfel de situații, actualizați Bitdefender pentru a vă asigura că aveți cele mai recente semnături malware și efectuați o scanare completă a sistemului pentru analizarea acestuia.

După finalizarea scanării, selectați acțiunii care doriți să fie aplicată în cazul elementelor infectate (dezinfectare, ștergere, mutare în carantină).

Avertisment

În cazul în care considerați că fișierul face parte din sistemul de operare Windows sau că nu este un fișier infectat, nu urmați acești pași și contactați serviciul de asistență clienți Bitdefender cât mai curând posibil.

Dacă acțiunea selectată nu a putut fi efectuată, iar jurnalul de scanare indică o infectare care nu a putut fi eliminată, trebuie să ștergeți fișierul/fișierele manual:

Prima metodă poate fi utilizată în modul normal:

1. Dezactivați protecția antivirus în timp real a Bitdefender:

a. Deschideți fereastra Bitdefender.

b. Faceți clic pe butonul **Setări** de pe bara de instrumente din partea superioară.

c. Selectați **Antivirus**.

d. Faceți clic pe secțiunea **Shield** din fereastra **Setări Antivirus**.

e. Faceți clic pe comutator pentru a dezactiva **scanarea la accesare**.

2. Afișați elementele ascunse din Windows. Pentru a afla cum să procedați, consultați *„Cum pot afișa elementele ascunse din Windows?"* (p. 58).
3. Mergeți la locația unde se găsește fișierul infectat (verificați jurnalul de scanare) și ștergeți-l.
4. Activați protecția antivirus în timp real a Bitdefender.

În cazul în care prima metodă nu a reușit să elimine infecția, urmați acești pași:

1. Reporniți sistemul în Safe Mode. Pentru a afla cum să procedați, consultați *„Cum pot să repornesc sistemul în Safe Mode?"* (p. 60).
2. Afișați elementele ascunse din Windows.
3. Mergeți la locația unde se găsește fișierul infectat (verificați jurnalul de scanare) și ștergeți-l.
4. Reporniți sistemul în mod normal.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului"* (p. 156).

26.3. Cum elimin un virus dintr-o arhivă?

O arhivă este un fișier sau o colecție de fișiere comprimate într-un format special, în scopul reducerii spațiului de pe hard-disc necesar stocării fișierelor.

Unele dintre aceste formate sunt formate deschise, ceea ce permite Bitdefender să scaneze în interiorul acestora și apoi să ia măsurile corespunzătoare pentru eliminarea infecțiilor.

Alte formate de arhivă sunt închise complet sau parțial, iar Bitdefender poate identifica numai prezența virușilor din acestea însă nu poate lua niciun fel de măsură în acest sens.

Dacă Bitdefender vă anunță că a fost detectat un virus într-o arhivă și nu este disponibilă nicio acțiune, aceasta înseamnă că eliminarea virusului nu este posibilă din cauza restricțiilor legate de setările referitoare la permisiunile arhivelor.

Iată cum puteți elimina un virus stocat într-o arhivă:

1. Identificați arhiva care conține virusul în urma unei scanări a sistemului.

2. Dezactivați protecția antivirus în timp real a Bitdefender:
   a. Deschideți fereastra Bitdefender.
   b. Faceți clic pe butonul **Setări** de pe bara de instrumente din partea superioară.
   c. Selectați **Antivirus**.
   d. Faceți clic pe secțiunea **Shield** din fereastra **Setări Antivirus**.
   e. Faceți clic pe comutator pentru a dezactiva **scanarea la accesare**.
3. Accesați locația arhivei și dezarhivați-o utilizând o aplicație de arhivare, cum ar fi WinZip.
4. Identificați fișierul infectat și ștergeți-l.
5. Ștergeți arhiva inițială pentru a vă asigura că fișierul infectat este eliminat în totalitate.
6. Recomprimați fișierele într-o nouă arhivă utilizând o aplicație de arhivare, cum ar fi WinZip.
7. Activați protecția antivirus în timp real a Bitdefender și executați o scanare completă a sistemului pentru a vă asigura că sistemul nu este infectat.

Notă
Este important de reținut faptul că un virus aflat într-o arhivă nu reprezintă o amenințare imediată la adresa sistemului dumneavoastră deoarece virusul trebuie să fie dezarhivat și executat pentru a putea infecta calculatorul.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 156).

26.4. Cum elimin un virus dintr-o arhivă de e-mail?

Bitdefender poate de asemenea să identifice viruși din bazele de date de e-mail și arhivele de e-mail stocate pe disc.

Uneori este necesară identificarea mesajului infectat utilizând informațiile puse la dispoziție în raportul de scanare și ștergerea acestuia în mod manual.

Iată cum puteți elimina un virus stocat într-o arhivă de e-mail:

1. Scanați baza de date de e-mail folosind Bitdefender.
2. Dezactivați protecția antivirus în timp real a Bitdefender:
   a. Deschideți fereastra Bitdefender.
   b. Faceți clic pe butonul **Setări** de pe bara de instrumente din partea superioară.
   c. Selectați **Antivirus**.
   d. Faceți clic pe secțiunea **Shield** din fereastra **Setări Antivirus**.

e. Faceți clic pe comutator pentru a dezactiva **scanarea la accesare**.

3. Deschideți raportul de scanare și utilizați informațiile de identificare (Subiect, De la, Către) aferente mesajelor infectate pentru a le localiza în clientul de e-mail.
4. Ștergeți mesajele infectate.Majoritatea clienților de e-mail mută mesajul șters într-un director de recuperare, de unde acesta poate fi recuperat.Trebuie să vă asigurați că mesajul este șters și din acest director de recuperare.
5. Arhivați directorul în care se află mesajul infectat.
   - În Outlook Express:În meniul File, faceți clic pe Folder și apoi pe Compact All Folders.
   - În Microsoft Outlook:În meniul File, faceți clic pe Data File Management.Selectați fișierele din directoarele personale (.pst) pe care intenționați să le compactați și faceți clic pe Settings.Faceți clic pe Compact.
6. Activați protecția antivirus în timp real a Bitdefender.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 156).

26.5. Ce trebuie să fac dacă suspectez că un fișier este periculos?

Există posibilitatea să considerați că un anumit fișier din sistemul dumneavoastră este periculos chiar dacă Bitdefender nu l-a detectat.

Pentru a vă asigura că sistemul dumneavoastră este protejat, urmați pașii de mai jos:

1. Executați o **scanare a sistemului** cu Bitdefender. Pentru a afla cum să procedați, consultați *„Cum îmi scanez sistemul?”* (p. 46).
2. Dacă procesul de scanare nu a detectat nimic, dar încă aveți dubii cu privire la fișier, contactați reprezentanții serviciul de asistență pentru ajutor.

   Pentru a afla cum să procedați, consultați *„Solicitarea ajutorului”* (p. 156).

26.6. Cum să curățați fișierele infectate din System Volume Information

Directorul System Volume Information se află într-o zonă a hard-discului creată de către sistemul de operare și utilizată de Windows pentru stocarea de informații critice referitoare la configurația sistemului.

Motoarele Bitdefender pot detecta orice fișiere infectate stocate de către System Volume Information, însă aceasta fiind o zonă protejată, fișierele nu pot fi șterse.

Fișierele infectate detectate în directoarele System Restore vor apărea în jurnalul de scanare după cum urmează:

`?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…`

Pentru a șterge complet și imediat fișierele infectate din locul unde sunt stocate, dezactivați și reactivați funcția System Restore.

Atunci când funcția System Restore este dezactivată, toate punctele de restaurare sunt șterse.

Atunci când funcția System Restore este activată din nou, sunt create noi puncte de restaurare conform programării și evenimentelor apărute.

Pentru a dezactiva funcția System Restore, urmați acești pași:

- **Pentru Windows XP:**
  1. Urmați această cale: **Start** → **All Programs** → **Accessories** → **System Tool** → **System Restore**
  2. Faceți clic pe **System Restore Settings** în partea stângă a ferestrei.
  3. Bifați căsuța **Turn off System Restore** pentru toate unitățile și faceți clic pe **Apply**.
  4. Atunci când sunteți avertizat că toate punctele de restaurare vor fi șterse, faceți clic pe **Yes** pentru a continua.
  5. Pentru a activa funcția System Restore, debifați căsuța **Turn off System Restore** pentru toate unitățile și faceți clic pe **Apply**.
- **Pentru Windows Vista:**
  1. Urmăriți această cale: **Start** → **Control Panel** → **System and Maintenance** → **System**
  2. În panoul stâng, faceți clic pe **System protection**.

     Dacă vi se solicită să introduceți o parolă de administrator sau să confirmați, introduceți parola sau confirmați.
  3. Pentru a dezactiva funcția System Restore, debifați căsuțele corespunzătoare fiecărei unități și faceți clic pe **OK**.
  4. Pentru a activa funcția System Restore, bifați căsuțele corespunzătoare fiecărei unități și faceți clic pe **OK**.
- **Pentru Windows 7:**
  1. Faceți clic pe **Start**, clic-dreapta pe **Computer** și alegeți **Properties**.
  2. Faceți clic pe linkul **System protection** din panoul stâng.
  3. Din opțiunile **System protection**, selectați fiecare literă de unitate și faceți clic pe **Configure**.

4. Selectați **Turn off system protection** și faceți clic pe **Apply**.
5. Faceți clic pe **Ștergere**, apoi pe **Continuare** atunci când vi se solicită acest lucru și ulterior pe **OK**.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați Bitdefender pentru asistență, așa cum se arată în secțiunea *„Solicitarea ajutorului”* (p. 156).

26.7. Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare?

Aceasta reprezintă doar o notificare referitoare la faptul că Bitdefender a detectat aceste fișiere ca fiind protejate fie prin parolă, fie cu o anumită formă de criptare.

Cel mai frecvent, elementele protejate prin parolă sunt următoarele:

- Fișiere care aparțin unei alte soluții de securitate.
- Fișiere care aparțin sistemului de operare.

Pentru a putea scana conținutul, aceste fișiere trebuie să fie extrase sau decriptate.

În cazul în care conținutul respectiv este extras, Bitdefender va scana automat conținutul pentru a vă proteja calculatorul. Dacă doriți să scanați acele fișiere folosind Bitdefender, trebuie să contactați producătorul produsului pentru a obține mai multe detalii despre respectivele fișiere.

Noi vă recomandăm să ignorați acele fișiere deoarece acestea nu reprezintă o amenințare pentru sistemul dumneavoastră.

26.8. Ce reprezintă elementele omise din jurnalul de scanare?

Toate fișierele care apar ca fiind omise în raportul de scanare nu conțin niciun fel de viruși.

Pentru performanțe sporite, Bitdefender nu scanează fișiere care nu au fost modificate de la ultima scanare.

26.9. Ce reprezintă fișierele supracomprimate din jurnalul de scanare?

Elementele supracomprimate sunt elemente care nu au putut fi extrase de către motorul de scanare sau elemente pentru care timpul necesar decriptării ar fi fost prea lung ducând la instabilitatea sistemului.

Comprimarea în exces se referă la faptul că Bitdefender a sărit peste scanarea respectivei arhive deoarece dezarhivarea acesteia s-a dovedit a consuma prea mult din resursele sistemului. Conținutul va fi scanat pe baza accesului în timp real, dacă este cazul.

26.10. De ce Bitdefender a șters în mod automat un fișier infectat?

În cazul în care este detectat un fișier infectat, Bitdefender va încerca în mod automat să-l dezinfecteze.Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

Pentru anumite tipuri de malware, dezinfecția nu este posibilă deoarece fișierul detectat este în întregime rău intenționat. În astfel de situații, fișierul infectat este șters de pe disk.

Acesta este cazul fișierelor de instalare care sunt descărcate de pe site-uri web nesigure.Dacă vă aflați într-o astfel de situație, descărcați fișierul de instalare de pe site-ul web al producătorului sau de pe un alt site web sigur.

Contactați-ne

27. Solicitarea ajutorului

Bitdefender se străduiește să ofere clienților săi un nivel neegalat în ceea ce privește rapiditatea și acuratețea suportului tehnic. Dacă vă confruntați cu o problemă sau aveți o întrebare referitoare la produsul Bitdefender deținut, puteți utiliza un număr de resurse online pentru a găsi rapid o soluție sau un răspuns. Sau, dacă preferați, puteți contacta echipa de Servicii clienți a Bitdefender. Reprezentanții noștri pentru suport tehnic vă vor răspunde la întrebări la timp și vă vor oferi asistența de care aveți nevoie.

Secțiunea *„Soluționarea problemelor frecvente”* (p. 131) vă oferă informațiile necesare referitoare la cele mai frecvent întâlnite probleme atunci când utilizați acest produs.

Dacă nu găsiți o soluție la problema dumneavoastră printre resursele puse la dispoziție, ne puteți contacta direct:

- „Contactați-ne direct din cadrul produsului dumneavoastră Bitdefender” (p. 156)
- „Contactați-ne prin intermediul Centrului nostru de asistență online” (p. 157)

Important

Pentru a contacta serviciul de asistență clienți Bitdefender, produsul dumneavoastră Bitdefender trebuie să fie înregistrat. Pentru mai multe informații, consultați *„Înregistrarea Bitdefender”* (p. 31).

Contactați-ne direct din cadrul produsului dumneavoastră Bitdefender

Dacă dispuneți de o conexiune la internet funcțională, puteți contacta Bitdefender pentru asistență direct din interfața produsului dumneavoastră.

Urmați acești pași:

1. Deschideți fereastra Bitdefender.
2. Faceți clic pe link-ul **Ajutor și asistență** din colțul dreapta jos al ferestrei.
3. Aveți la dispoziție următoarele opțiuni:
   - **Ajutor Bitdefender**.

     Răsfoiți articolele din documentația Bitdefender și soluțiile produse.
   - **Centrul de asistență**

     Accesați baza noastră de date și căutați informațiile necesare.
   - **Contactați serviciul de asistență**

     Cu ajutorul butonului **Contactare asistență** pentru a lansa Instrumentul de asistență și pentru a contacta Serviciul de asistență clienți. Puteți naviga prin

programul asistent cu ajutorul butonului **Înainte**. Pentru a părăsi asistentul, faceți clic pe **Anulează**.

a. Selectați căsuța de acceptare și faceți clic pe **Înainte**.

b. Completați formularul cu datele necesare:

i. Introduceți adresa dumneavoastră de e-mail.

ii. Introduceți numele complet.

iii. Alegeți-vă țara din meniul corespunzător.

iv. Introduceți o descriere a problemei întâmpinate.

c. Vă rugăm să așteptați câteva minute pentru ca Bitdefender să adune informații referitoare la produs. Aceste informații îi vor ajuta pe inginerii noștri să găsească o soluție la problema dumneavoastră.

d. Faceți clic pe **Finalizare** pentru a transmite informațiile la Departamentul de asistență clienți Bitdefender. Veți fi contactat cât mai curând posibil.

Contactați-ne prin intermediul Centrului nostru de asistență online

Dacă nu puteți accesa informațiile necesare utilizând produsul Bitdefender, consultați Centrul nostru online de asistență:

1. Mergeți la http://www.bitdefender.ro/support/consumer.html. Centrul de asistență Bitdefender include numeroase articole care cuprind soluții la problemele asociate Bitdefender.
2. Selectați produsul dumneavoastră și căutați în Centrul de asistență Bitdefender articole care vă pot ajuta să soluționați problema.
3. Citiți articolele sau documentele relevante și încercați soluțiile propuse.
4. Dacă soluția propusă nu vă ajută să rezolvați problema, mergeți la http://www.bitdefender.ro/support/contact-us.html și luați legătura cu reprezentații serviciului de asistență.

28. Resurse online

Sunt disponibile mai multe resurse online pentru a vă ajuta la soluționarea problemelor și întrebărilor referitoare la produsul Bitdefender.

- Centrul de asistență Bitdefender:http://www.bitdefender.ro/support/consumer.html
- Forumul de suport al Bitdefender:http://forum.bitdefender.com
- Portalul de securitate informatică HOTforSecurity:http://www.hotforsecurity.com

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare privind securitatea calculatoarelor, produsele și compania Bitdefender.

28.1. Centrul de asistență Bitdefender

Centrul de asistență Bitdefender este un depozit online ce conține informații despre produsele Bitdefender. Acesta stochează, într-un format ușor accesibil, rapoarte privind rezultatele unor activități continue de asistență tehnică și remediere ale echipelor de asistență și dezvoltare Bitdefender, alături de articole mai generale referitoare la prevenirea virușilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Centrul de asistență Bitdefender este deschis publicului și pot fi realizate căutări în mod liber. Prin intermediul informațiilor extinse pe care le conține, putem oferi clienților Bitdefender cunoștințele tehnice și înțelegerea de care au nevoie. Toate solicitările valide pentru informații sau rapoartele de eroare care vin din partea clienților Bitdefender ajung la Serviciul de asistență Bitdefender sub formă de rapoarte de remediere a erorilor, notițe de evitare a erorilor, articole informaționale pentru a completa fișierele de ajutor ale produsului.

Centrul de asistență Bitdefender este disponibil oricând la http://www.bitdefender.ro/support/consumer.html.

28.2. Forumul de suport al Bitdefender

Forumul de suport al Bitdefender le oferă utilizatorilor Bitdefender o modalitate facilă de a obține ajutor și de a-i ajuta pe alții.

În cazul în care produsul dumneavoastră Bitdefender nu funcționează bine, nu poate înlătura anumiți viruși de pe calculator sau dacă aveți întrebări referitoare la modul de funcționare, postați problema sau întrebarea pe forum.

Tehnicienii suport ai Bitdefender monitorizează forumul pentru a verifica noile postări cu scopul de a vă ajuta. De asemenea, puteți obține un răspuns sau o soluție de la un utilizator Bitdefender cu mai multă experiență.

Înainte de a posta problema sau întrebarea, sunteți rugat să verificați în forum existența unui subiect similar sau corelat.

Forumul de suport al Bitdefender este disponibil la http://forum.bitdefender.com, în 5 limbi diferite: engleză, germană, franceză, spaniolă și română. Faceți clic pe linkul **Home & Home Office Protection** pentru a accesa secțiunea dedicată produselor pentru consumatori individuali.

28.3. Portalul HOTforSecurity

Portalul HOTforSecurity reprezintă o sursă bogată de informații referitoare la securitatea calculatoarelor. Aici puteți afla informații despre diverse pericole la care se expune computerul dvs. atunci când este conectat la Internet (malware, phishing, spam, infracțiuni cibernetice). Un dicționar util vă ajută la înțelegerea termenilor de securitate a calculatoarelor cu care nu sunteți familiarizați.

Se postează în mod regulat noi articole pentru a vă ține la curent cu cele mai recente pericole descoperite, tendințele actuale din domeniul securității și alte informații din domeniul securității calculatoarelor.

Vizitați pagina de web HOTforSecurity accesând http://www.hotforsecurity.com.

29. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 10 ani BitDefender a câștigat o reputație indisputabilă în depășirea așteptărilor clienților și partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

29.1. Adrese web

Departament de vânzări: sales@bitdefender.ro
Centrul de asistență: http://www.bitdefender.ro/site/contact/1/
Documentație: documentation@bitdefender.com
Distribuitori locali:http://www.bitdefender.ro/partners
Program de Parteneriat: partners@bitdefender.com
Relații media: pr@bitdefender.com
Cariere: jobs@bitdefender.com
Subscrieri viruși: virus_submission@bitdefender.com
Subscrieri spam: spam_submission@bitdefender.com
Raportare abuz: abuse@bitdefender.com
Site web:http://www.bitdefender.ro

29.2. Distribuitori locali

Distribuitorii locali Bitdefender sunt pregătiți să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale.

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

1. Mergeți la http://www.bitdefender.ro/partners/#Partner Locator/.
2. Datele de contact ale distribuitorilor locali Bitdefender ar trebui să se afișeze automat. În caz contrar, selectați țara de reședință pentru a accesa aceste informații.
3. În cazul în care nu găsiți un distribuitor Bitdefender în țara dumneavoastră, nu ezitați să ne contactați prin e-mail la adresa sales@bitdefender.com. Vă rugăm să scrieți mesajul în engleză pentru a ne da posibilitatea să vă ajutăm cu promptitudine.

29.3. Filialele Bitdefender

Reprezentanțele Bitdefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și cele generale. Adresele lor precum și modul în care pot fi contactate sunt date mai jos.

U.S.A

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefon (birou&vânzări): 1-954-776-6262
Vânzări: sales@bitdefender.com
Suport tehnic: http://www.bitdefender.com/help
Web: http://www.bitdefender.com

Marea Britanie și Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-mail: info@bitdefender.co.uk
Telefon: +44 (0) 8451-305096
Vânzări: sales@bitdefender.co.uk
Suport tehnic: http://www.bitdefender.com/help
Web: http://www.bitdefender.co.uk

Germania

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Birou: +49 2301 91 84 0
Vânzări: vertrieb@bitdefender.de
Suport tehnic: http://kb.bitdefender.de
Web: http://www.bitdefender.de

Spania

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Vânzări: comercial@bitdefender.es
Suport tehnic: http://www.bitdefender.es/ayuda
Site web: http://www.bitdefender.es

România

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefon vânzări: +40 21 2063470
E-mail vânzări: sales@bitdefender.ro
Suport tehnic: http://www.bitdefender.ro/suport
Site web: http://www.bitdefender.ro

Emiratele Arabe Unite

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefon vânzări: 00971-4-4588935 / 00971-4-4589186
E-mail vânzări: sales@bitdefender.com
Suport tehnic: http://www.bitdefender.com/suport
Site web: http://www.bitdefender.com/world

Vocabular

ActiveX

ActiveX este un mod de scriere a programelor astfel încât să poată fi apelate de celelalte programe și sisteme de operare. Tehnologia ActiveX este utilizată pentru realizarea de pagini Web interactive care se comportă ca niște aplicații și nu ca niște simple pagini statice. Cu elemente de ActiveX, utilizatorii pot răspunde la întrebări, să utilizeze butoane și să interacționeze și în alte moduri cu pagina Web. Controalele ActiveX sunt adesea scrise utilizând limbajul Visual Basic.

Active X este cunoscut pentru lipsa totală de control al securității; experții în securitatea calculatoarelor descurajează utilizarea lui pe Internet.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteți instala actualizarea.

Bitdefender dispune de modulul său propriu care realizează actualizarea automatică sau manuală.

Adware

Aplicația adware este adesea combinată cu o aplicație gazdă care este oferită gratuit dacă utilizatorul acceptă aplicația adware. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licențiere care explică scopul aplicației, nu este comisă nicio infracțiune.

Totuși, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanțele sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licențiere.

Applet-uri Java

Reprezintă un program Java care este proiectat să ruleze doar pe pagini web. Pentru a utiliza un applet pe o pagină web, trebuie specificate numele applet-ului și mărimea acestuia. Când este accesată o pagină web, browser-ul descarcă applet-ul de pe un server și îl rulează pe mașina utilizatorului (clientul). Applet-urile diferă de aplicații prin aceea că sunt guvernate de un protocol de securitate strict.

Astfel că, deși pot rula pe calculatorul unui utilizator, ele nu pot citi sau scrie date pe aceste calculatoare. Applet-urile sunt restricționate de domeniul de care aparțin în ceea ce privește scrierea și citirea datelor.

Arhivă

Un disc, o casetă sau un director care conține fișiere de rezervă.

Un fișier care conține unul sau mai multe fișiere într-un format comprimat.

Backdoor

Reprezintă o breșă de securitate realizată în mod deliberat. Motivația acestor "găuri" nu este întotdeauna malițioasă: unele sisteme de operare, de exemplu, sunt puse în circulație cu conturi privilegiate pentru tehnicienii din service sau de responsabilii cu mentenanță produsului din partea vânzătorului.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în bara de sarcini Windows (de obicei în partea de jos, lângă ceas) și conține pictograme miniaturale pentru accesul rapid la aplicații de sistem cum ar fi cele legate de fax, imprimantă, modem, volum și altele. Faceți dublu-clic sau clic dreapta cu mouse-ul pe o pictogramă pentru a vizualiza și accesa detaliile și comenzile.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza și încărca pagini de Web. Două din cele mai populare browsere sunt Mozilla Firefox și Microsoft Internet Explorer. Ambele sunt browsere grafice, ceea ce înseamnă că pot afișa atât grafice cât și text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet și animație.

Cale

Reprezintă direcția exactă către un fișier de pe un calculator. Această direcție este specificată utilizând sistemul ierarhic de organizare a fișierelor de sus în jos.

Ruta între două puncte, cum ar fi de exemplu canalul de comunicație între două computere.

Client de mail

Un client de mail este o aplicație care vă permite să trimiteți și să recepționați mesaje.

Cookie

În domeniul Internetului, cookie-urile reprezintă mici fișiere ce conțin informații despre fiecare calculator care pot fi analizate și folosite de către cei care publică reclame pentru a vă urmări interesele și preferințele online. În acest domeniu, tehnologia cookie-urilor este în curs de dezvoltare, iar intenția este de a afișa direct acele anunțuri care corespund intereselor dumneavoastră. Această facilitate are avantaje și dezavantaje pentru mulți deoarece, pe de o parte, este eficientă și pertinentă din moment ce vizualizați doar acele anunțuri despre

subiecte care vă interesează. Pe de altă parte, cookie-urile implică de fapt o "monitorizare" și "urmărire" a site-urilor vizitate și a link-urilor accesate. Astfel, în mod logic, părerile sunt împărțite în ceea ce privește confidențialitatea și mulți se simt jigniți de faptul că sunt văzuți ca un simplu "număr SKU" (este vorba de codul de bare de pe spatele ambalajelor care este scanat pe bandă la supermarket). Deși acest punct de vedere poate fi considerat extrem, în anumite cazuri el reprezintă chiar ceea ce se întâmplă în realitate.

Descărcare

Reprezintă copierea (de obicei a unui întreg fișier) de pe o sursă principală pe un dispozitiv periferic. Termenul este adesea utilizat pentru a descrie procesul de copiere a unui fișier de pe un serviciu on-line pe calculatorul unui utilizator. De asemenea se mai poate referi și la copierea unui fișier de pe un server de rețea pe un calculator din rețea.

Drive de disc

Este un dispozitiv care citește date de pe un disc și scrie date pe un disc.

Un drive de hard disc citește / scrie date de pe / pe hard disc.

Un drive de floppy accesează dischetele floppy.

Drive-ele de disc pot fi sau interne (incorporate în interiorul unui calculator) sau externe (plasate într-o locație separată care este conectată la calculator).

E-mail

Se referă la poșta electronică. Acesta este un serviciu care transmite mesaje către alte calculatoare prin intermediul rețelei locale sau globale.

Elemente din startup

Orice fișier plasat în acest director se va deschide de fiecare dată când calculatorul este pornit. De exemplu, un sunet care se va auzi atunci când este pornit calculatorul sau chiar aplicații sunt considerate elemente de startup. În mod normal, un alias al programului este plasat în acest director, și nu direct fișierul.

Evenimente

O acțiune sau întâmplare detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi executarea unui clic cu mouse-ul sau apăsarea unei taste, sau întâmplări în sistem cum ar fi epuizarea memoriei.

Extensie de fișier

Reprezintă porțiunea dintr-un nume de fișier ce urmează după caracterul punct, și care indică tipul de date pe care le stochează fișierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fișiere. De obicei aceasta este formată din una până la trei litere (unele

sisteme de operare mai vechi nu suportă mai mult de trei). De exemplu: "c" pentru fișierele sursă scrise în limbajul C, "ps" pentru fișiere PostScript sau "txt" pentru fișierele text oarecare.

Fals pozitiv

Apare atunci când un analizator detectează un fișier ca fiind infectat când de fapt acesta nu este infectat.

Fișier de raport

Reprezintă un fișier care listează acțiunile care au avut loc. Bitdefender menține un fișier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fișierelor, numărul de arhive și fișiere scanate, câte fișiere infectate și suspecte au fost găsite.

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât și reasamblarea pachetelor IP.

Keylogger

Un keylogger este o aplicație care înregistrează orice tastați.

Keyloggerele nu au o natură periculoasă. Pot fi folosite în scopuri legitime, cum ar fi monitorizarea angajaților sau a activității copiilor. Cu toate acestea, utilizarea lor de către infractorii cibernetici în scopuri negative este din ce în ce mai răspândită (de exemplu, pentru colectarea informațiilor cu caracter privat, cum ar fi acreditările de înregistrare și codurile numerice personale).

Linie de comandă

Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Memorie

Reprezintă arii de stocare a datelor din interiorul calculatorului. Termenul de memorie desemnează locul de stocare a datelor pe chipuri și pe cel al cuvintelor pe casete sau cd-uri audio. Fiecare calculator dispune de o anumită capacitate de memorie fizică, referită de obicei prin memorie principală sau RAM.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruși noi. Această metodă de scanare nu se bazează pe semnături de viruși cunoscuți. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuși ocazional poate raporta un cod suspicios în programe normale, generând așa-numitul "fals pozitiv".

Metoda ne-euristică

Această metodă de scanare se bazează pe semnături de viruși cunoscuți. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus și din acest motiv nu generează fals pozitiv.

Phishing

Reprezintă acțiunea de a trimite un e-mail către un utilizator, pretinzând a fi o companie legitimă, în încercarea de a păcăli utilizatorul să furnizeze informații confidențiale ce vor fi folosite la furtul identității. E-mailul îndreaptă utilizatorul către un site Web unde acesta este rugat să actualizeze informații personale, cum ar fi parole și numere de card de credit, de asigurări sociale și de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals și folosit pentru a fura informațiile despre utilizator.

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Există porturi interne pentru conectarea hard discurilor, monitoarelor și tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului, și a altor dispozitive periferice.

În rețelele TCP / IP și UDP acestea reprezintă un punct terminus al unei conexiuni logice. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Programe împachetate

Reprezintă un fișier în format comprimat. Multe dintre sistemele de operare și aplicații conțin comenzi care vă dau posibilitatea de a arhiva un fișier astfel încât să ocupe mai putină memorie. De exemplu, să presupunem că aveți un fișier text care conține zece caractere reprezentând spații. În mod normal, acesta ar necesita zece biți de memorie pentru a fi stocați.

Totuși, un program care arhivează fișiere va înlocui caracterele de spațiu printr-un caracter special reprezentând spațiu, urmat de un număr care reprezintă numărul de spații înlocuite. În acest caz, cele zece caractere reprezentând spațiu ar necesita doar doi biți. Aceasta este doar un exemplu de comprimare - există multe alte metode în afară de aceasta.

Rootkit

Un rootkit este un set de unelte soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX și se referea la unelte recompilate ce furnizau intrușilor drepturi administrative, permițându-le să își ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fișiere, loginuri și jurnale. Acestea pot de asemenea să intercepteze date de la terminale, conexiuni la rețea sau perifice dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele și chiar unele aplicații ascunde fișiere critice utilizând rootkituri. Totuși, ele sunt folosite în general pentru a ascunde aplicații malițioase sau prezența intrușilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea și integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fișiere și jurnale și evita detecția.

Script

Un alt termen pentru fișiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

Sector de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului și altele). În cazul discurilor de startup, sectorul de boot conține un program care încarcă sistemul de operare.

Semnătură virus

Reprezintă tiparul binar al unui virus, utilizat de un program antivirus pentru detecția și eliminarea virusului.

Spam

Termen ce acoperă întreaga gamă a mesajelor electronice nesolicitate (junk). În general, acestea sunt cunoscute sub numele de mesaje electronice nesolicitate.

Spyware

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la Internet fără știrea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei primite ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuși, trebuie știut că majoritatea aplicațiilor de tip shareware și freeware nu conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet și transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail și chiar parole și numere de carduri de credit.

Asemănarea dintre spyware și un cal troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obișnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fișiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică și intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât și a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la Internet a utilizatorului. Deoarece folosesc memorie și resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul Internet și care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware și sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât și convenții folosite în conectarea rețelelor și rutării traficului.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruși, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascați troieni este acela care pretinde că elimină virușii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruși pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă dușmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul orașului lor, din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraș și să captureze Troia.

Vierme

Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.

Virus

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără știrea dumneavoastră și rulează independent de voința dumneavoastră. Cea mai mare parte a virușilor se pot și înmulți. Toți virușii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar și un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus și mai periculos este acela care este capabil să se răspândească în rețea și poate să treacă de sistemele de securitate.

Virus de boot

Reprezintă un virus care infectează sectorul de boot al unui disc fix sau al unei dischete. Orice încercare de a face boot de pe o dischetă infectată cu un virus de boot va determina virusul să devină activ în memorie. Din acest moment

de fiecare dată când veți realiza boot-area sistemului, virusul va deveni activ în memorie.

Virus de macro

Un tip de virus informatic este acela inclus ca macro într-un document. Multe aplicații cum ar fi de exemplu Microsoft Word și Excel suportă limbaje macro puternice.

Aceste limbaje permit încapsularea de macro-uri în documente și execută aceste macro-uri de fiecare dată când este deschis documentul.

Virus polimorf

Reprezintă un virus care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruși sunt greu de identificat.