GHIDUL UTILIZATORULUI

Bitdefender CONSUMER SOLUTIONS

Ultimate Small Business Security

Bitdefender Ultimate Small Business Security

Ghidul utilizatorului

Publication date 05/31/2024

Aviz juridic

Bitdefender

Cuprins

DESPRE ACEST GHID

Scopul și publicul vizat

Bitdefender Ultimate Small Business Security este un pachet de abonament cu mai multe abonamente, conceput pentru a satisface nevoile de securitate cibernetică ale întreprinderilor mici. Cu un set cuprinzător de caracteristici, integrare dedicată și instrumente de management intuitive, proprietarii de întreprinderi mici își pot proteja activele digitale fără expertiză IT sau securitate cibernetică.

Planul oferă protecție cuprinzătoare special concepută pentru companiile mici, inclusiv:

- **Protecția dispozitivului multiplatformă:** Protejează-ți toate dispozitivele, de la computere la telefoane mobile și servere.
- **Gestionare ușoară:** Mențineți siguranța echipei și a operațiunilor de afaceri fără efort.
- **Protecția activelor comerciale și a reputației:** Asigurați cel mai înalt nivel de protecție pentru afacerea dvs. prin prevenirea asocierii cu activități frauduloase.
- **Configurare simplificată:** Procesul de onboarding simplifică configurarea pentru utilizatorii non-tehnici, asigurând o configurație lină și sigură.

Cum să utilizați acest ghid

Acest ghid este organizat în jurul celor patru produse incluse în Bitdefender Total Security:

- Securitate totală pentru PC (pagina 9)
  Aflați cum să utilizați produsul pe computerele și laptopurile bazate pe Windows.
- Antivirus pentru Mac (pagina 151)
  Aflați cum să utilizați produsul pe Mac-urile dvs.
- Securitate mobilă pentru Android (pagina 184)
  Aflați cum să utilizați produsul pe smartphone-urile și tabletele bazate pe Android.

- Securitate mobilă pentru iOS (pagina 218)
  Aflați cum să utilizați produsul pe smartphone-urile și tabletele dvs. bazate pe iOS.
- VPN (pagina 234)
  Aflați cum să vă ascundeți identitatea online folosind Bitdefender VPN pe oricare dintre dispozitivele dvs.
- Manager de parole (pagina 257)
  Urmăriți și stocați în siguranță toate parolele și acreditările dvs. cu Password Manager.
- Protecția identității digitale (pagina 282)
  Aflați cum să gestionați corect protecția identității digitale.
- Obține ajutor (pagina 290)
  Aflați unde să căutați ajutor dacă apare ceva neașteptat.

Convenții utilizate în acest ghid

Convenții tipografice

Manualul conține diferite stiluri de text, pentru o lectură cât mai ușoară. Aspectul și semnificația acestora sunt prezentate în tabelul de mai jos.

Aspect	Descriere
sample syntax	Exemplele de sintaxă sunt imprimate cu caractere monospaced.
https://www.bitdefender.com	Linkurile URL indică locații externe, pe serverele http sau ftp.
documentation@bitdefender.com	Adresele de e-mail sunt inserate în text ca informație de contact.
Despre acest Ghid (pagina 1)	Acesta este un link intern, care vă direcționează către o locație din document.
filename	Fișierul și directoarele sunt tipărite folosind monospaced font.
opțiune	Toate opțiunile de produs sunt imprimate folosind caractere **îngroșate**.
cuvânt cheie	Cuvintele cheie sau expresiile importante sunt evidențiate folosind caractere **îngroșate**.

Atenționări

Atenționările sunt note din text, marcate grafic, care oferă informații suplimentare legate de paragraful respectiv.

Nota

Nota este o scurtă observație. Deși pot fi omise, notele pot furniza informații importante, cum ar fi o caracteristică specifică sau un link către un subiect relevant.

Important

Segmentele marcate astfel necesită atenția ta și nu este recomandat să le omiți. De obicei, aici sunt furnizate informații importante, dar nu esențiale.

Avertizare

Acestea sunt informații esențiale, care trebuie tratate cu o atenție deosebită. Dacă urmezi indicațiile, nu se va întâmpla nimic rău. Este recomandat să citești și să înțelegi despre ce este vorba, deoarece aici se descrie ceva extrem de riscant.

Comentarii

Te invităm să participi la procesul de îmbunătățire al manualului. Toate informațiile prezentate au fost testate și verificate în mod riguros. Te rugăm să ne scrii despre orice inexactități pe care le vei găsi în acest manual, precum și să propui moduri prin care îl putem îmbunătăți, astfel încât să îți putem furniza o documentație ireproșabilă.

Anunțați-ne trimițând un e-mail la documentation@bitdefender.com. Scrieți toate e-mailurile dvs. legate de documentație în engleză, astfel încât să le putem procesa eficient.

1. CUM SĂ-ȚI CONFIGUREZI ABONAMENTUL

Primii pași în utilizarea abonamentului tău **Bitdefender Ultimate Small Business Security** au fost special gândiți pentru a asigura un proces rapid și ușor de inițiere, fără să fie nevoie de cunoștințe de IT sau securitate cibernetică. Va trebui să întreprinzi următoarele acțiuni:

1. **să activezi Bitdefender Ultimate Small Business Security:**
   Poți face asta urmând instrucțiunile din e-mailul de confirmare primit la achiziționarea produsului.
2. **Configurează-ți contul de business:**
   La activare, ți se va solicita să introduci denumirea companiei tale. Această informație va fi utilizată numai în scop de identificare și va fi afișată în diferite locuri din interfață. Reține că poți utiliza orice denumire dorești, nefiind necesară validarea ei.
3. **Alege-ți rolul în cadrul organizației:**
   - **Deținătorul companiei:**dacă tu ești deținătorul companiei și te ocupi de achiziții și configurare, selectează această opțiune.
   - **Administratorul de securitate:** dacă tu ești responsabil cu administrarea securității în cadrul companiei, alege această opțiune.

     Reține
     Administratorul de securitate are drepturi de acces similare cu cele ale deținătorului companiei, cu excepția operațiunilor de achiziție.

4. **Invită membrii echipei să își creeze conturi:**
   După ce ai introdus denumirea și ți-ai ales rolul, vei vedea o prezentare generală a abonamentului tău Bitdefender. De aici, poți alege să partajezi planul cu alți membri ai echipei sau să continui cu propria configurare, urmând procedurile de instalare adecvate pentru dispozitivul pe care dorești să instalezi Bitdefender, fiecare dintre acestea fiind prezentate în capitolul corespunzător din acest document.

> **Important**
> Îți recomandăm să începi prin a invita angajații înainte de a trece la procedurile de instalare.

5. **Selectează rolurile membrilor echipei:**
   Selectează rolurile angajaților pe care îi inviți să beneficieze de planul de securitate al companiei tale. Îi poți invita în calitate de:
   - **Administrator de securitate:** acest rol implică gestionarea membrilor, a dispozitivelor și a operațiunilor de securitate și este destinat angajaților care au un anumit nivel de cunoștințe în domeniul IT, fiind însărcinați cu gestionarea și monitorizarea aspectelor de securitate cibernetică ale companiei tale.
   - **Angajat:** angajații au vizibilitate și capacități de gestionare limitate. Aceștia vor avea nevoie de un cont Bitdefender Central pentru a-și proteja propriile dispozitive, în timp ce cei cu rolul **Administrator de securitate** pot supraveghea protecția și gestiona dispozitivele de la distanță.

6. **Trimite invitații prin e-mail către membrii echipei:**
   Introdu adresele de e-mail ale angajaților cu care vrei să partajezi planul Bitdefender. Poți trimite mai multe invitații în același timp.

   > **Reține**
   > Membrii invitați vor primi o invitație prin e-mail, indiferent de rolul pe care îl au. Ei trebuie să facă clic pe butonul **Activează în Bitdefender Central** și să accepte invitația folosind aceeași adresă de e-mail la care au primit invitația.

7. **Adaugă informațiile sensibile ale companiei care urmează să fie monitorizate:**
   Acum va trebui să configurezi monitorizarea expunerii activelor companiei, acesta fiind ultimul pas în acest proces.

   > **Reține**
   > **Expunerea resurselor companiei** este un serviciu disponibil numai pentru rolurile de administrator. (**Administrator de securitate** și **Deținătorul companiei**)

   Această caracteristică verifică expunerea datelor la nivel de companie pentru a proteja reputația companiei și pentru a preveni eventualele atacuri targetate.

- Din meniul din stânga al contului tău Bitdefender Central, navighează la secțiunea **Activitate business**.
- Fă clic pe butonul **Accesează setările de configurare** din panoul **Expunerea resurselor companiei**.
- Adaugă informațiile companiei:
  - Adresă de e-mail de serviciu
  - Card bancar companie
  - Conturi de pe rețelele de socializare
- După ce ai efectuat toate acțiunile sugerate, fă clic pe butonul **Marchează ca finalizat** pentru a confirma finalizarea și pentru a urmări progresul.

Odată ce ai finalizat acești pași, poți începe să configurezi **Bitdefender Ultimate Small Business Security**:

- Instalează pe dispozitive Windows: Instalare (pagina 9)
- Instalează pe dispozitive macOS: Instalarea Bitdefender Antivirus for Mac (pagina 152)
- Instalează pe dispozitive mobile Android: Instalarea Bitdefender Mobile Security (pagina 184)
- Instalează pe dispozitivele mobile iOS: Instalare Bitdefender Mobile Security for iOS (pagina 219)
- Instalează Bitdefender VPN pe dispozitivele tale: Instalarea Bitdefender Password Manager (pagina 236)
- Configurează Password Manager: Instalare (pagina 259)
- Configurează Digital Identity Protection: Configurați protecția identității digitale (pagina 283)

Continuarea acestui proces marchează activarea și configurarea cu succes a **Bitdefender Ultimate Small Business Security** pentru compania ta.

2. EXPUNEREA RESURSELOR COMPANIEI

Expunerea resurselor companiei este un serviciu Bitdefender Ultimate Small Business Security gestionat de administratori (deținătorul companiei și administratorul de securitate) care oferă vizibilitate în ceea ce privește expunerea informațiilor cheie ale companiei în urma breșelor de securitate a datelor. Serviciul Expunerea resurselor companiei monitorizează 3 componente pentru a detecta breșele de securitate a datelor:

- Adresă de e-mail de serviciu
- Card bancar companie
- Conturi de pe rețelele de socializare

De ce este important să monitorizați resursele companiei:

- **Pentru a proteja reputația:** previne orice prejudicii care ar putea afecta reputația companiei tale, remediind cu promptitudine efectele unei breșe de securitate.
- **Pentru siguranța angajaților:** protejează angajații împotriva atacurilor de phishing și a altor atacuri de inginerie socială prin monitorizarea și gestionarea datelor lor expuse.
- **Pentru a preveni atacurile targetate:** limitează potențialul pentru atacuri targetate, asigurându-se că informațiile sensibile rămân în siguranță.

După ce ai configurat detaliile serviciului **Expunerea resurselor companiei** în cadrul procesului **Cum să-ți configurezi abonamentul (pagina 4)** , poți**verifica rezultatele și poți lua măsuri în funcție de recomandări:**

Sistemul te va informa cu privire la orice breșe de securitate care implică aceste active monitorizate, inclusiv serviciile compromise și tipurile de informații expuse (de exemplu, adrese de e-mail, nume de utilizator, parole, locații geografice). Nu sunt afișate detalii specifice, ci doar categoriile de date expuse.

Pentru fiecare componentă monitorizată (e-mail de serviciu, cardul bancar al companiei, conturi pe rețelele de socializare), aplică recomandările de securitate furnizate. Acțiunile sugerate pot include:

- să le soliciți angajaților să își monitorizeze adresele de e-mail de serviciu cu ajutorul Bitdefender Digital Identity Protection;
- să schimbi parolele de pe site-urile web compromise și să le recomanzi angajaților să folosească Bitdefender Password Manager;
- să te asiguri că angajații instalează soluții de securitate Bitdefender pe toate dispozitivele pentru a preveni orice atac cibernetic;
- să le recomanzi angajaților să utilizeze Scam Copilot pentru a obține sfaturi privind posibilele scamuri și practicile de prevenire a fraudelor.
- să monitorizezi tranzacțiile și să schimbi cardului bancar, contactând banca emitentă.
- Activarea autentificării în doi pași pe platformele de socializare pentru a preveni autentificarea neautorizată.

> **Reține**
> După ce ai implementat acțiunile sugerate, trebuie să faci clic pe butonul **Marchează ca finalizat** pentru a confirma finalizarea și pentru a urmări progresul.

Prin aplicarea acestor pași, administratorii pot monitoriza și proteja cu ușurință compania împotriva riscurilor de expunere a datelor utilizând serviciul **Expunerea resurselor companiei**.

3. SECURITATE TOTALĂ PENTRU PC

3.1. Instalare

3.1.1. Pregătirea pentru instalare

Pentru a instala Bitdefender Ultimate Small Business Security fără probleme, trebuie sa parcurgi acești pași prealabili:

- Asigurați-vă dacă dispozitivul pe care doriți să instalați Bitdefender îndeplinește cerințele de sistem. În cazul în care dispozitivul nu întrunește toate cerințele 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, consultă Cerințe de sistem (pagina 9).
- Autentifica-te pe dispozitiv cu datele unui cont de administrator.
- Dezinstalează orice alt program similar de pe dispozitiv. Dacă se detectează ceva în timpul procesului de instalare Bitdefender, vei primi o notificare de dezinstalare. 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.
- Dezactivează sau dezinstalează orice alt program firewall de pe dispozitiv. 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, dispozitivul tău să fie conectat la internet, chiar atunci când instalarea se face 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.

3.1.2. Cerințe de sistem

Poți instala Bitdefender Ultimate Small Business Security doar pe dispozitive pe care rulează următoarele sisteme de operare:

- Windows 7 cu Service Pack 1

- Windows 8.1
- Windows 10
- 2,5 GB spațiu liber disponibil pe hard disk (cel puțin 800 MB pe unitatea de sistem)
- 2 GB de memorie (RAM)

De asemenea, puteți instala și rula Bitdefender Ultimate Small Business Security pe următoarele:

- Windows Server 2016 (cu experiență desktop):
  - Standard/RTM
  - Esențiale
  - Centru de date
- Windows Server 2019 (cu experiență desktop):
  - Standard/RTM
  - Esențial
  - Centru de date
- Windows Server 2022 (cu experiență desktop):
  - Standard/RTM
  - Centru de date

Important

* Performanța sistemului poate fi afectată pe dispozitivele care au procesoare de generație mai veche.

Notă

Pentru a afla pe ce sistem de operare funcționează dispozitivul tău și informațiile referitoare la hardware:

- În **Windows 7** fă clic dreapta pe **Computerul meu** de pe desktop și apoi selectează **Proprietăți** din meniu.
- În **Windows 8**, din ecranul de start, identifică **Computer** (de exemplu, poți începe să tastezi „Computer” direct în ecranul Start), apoi fă clic dreapta pe pictograma sa. În **Windows 8.1**, identifică **Acest PC**.

  Selectează **Proprietăți** din meniul din partea de jos. Caută în zona **Sistem** pentru a afla informații referitoare la tipul de sistem.
- În **Windows 10**, tastează **Sistem** în câmpul de căutare din bara de activități și apoi fă clic pe pictograma sa. Consultă zona **Sistem** pentru a afla informații despre tipul tău de sistem.

3.1.3. Cerințe software

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

- Microsoft Edge 40 sau superior
- Internet Explorer 10 sau o variantă mai recentă
- Mozilla Firefox 51 și o versiune mai recentă
- Google Chrome 34 și o versiune mai recentă
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 sau mai recent

3.1.4. Instalarea produsului dumneavoastră Bitdefender

Poți instala Bitdefender folosind CD-ul de instalare sau aplicația web descărcată pe dispozitivul tău **Bitdefender Central**.

Dacă produsul achiziționat acoperă mai multe dispozitive, repetă procesul de instalare și activează produsul utilizând același cont pe fiecare dispozitiv. Contul pe care trebuie să îl utilizezi este cel care conține abonamentul tău activ Bitdefender.

Instalare din Bitdefender Central

Din Bitdefender Central puteți descărca kitul de instalare corespunzător abonamentului achiziționat. Odată ce procesul de instalare s-a finalizat, Bitdefender Ultimate Small Business Security este dezactivat.

Pentru a descărca Bitdefender Ultimate Small Business Security din Bitdefender Central:

1. Accesează **Bitdefender Central**.
2. Accesează secțiunea **Dispozitivele mele** și apoi apasă pe **INSTALEAZĂ PROTECȚIA**.
3. Alege una dintre cele doua opțiuni disponibile:
   - **Protejează acest dispozitiv**
     a. Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
     b. Salvează fișierul de instalare.
   - **Protejează alte dispozitive**
     a. Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
     b. Apăsați pe **TRIMITE LINK DE DESCĂRCARE**.
     c. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**.
     Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.
     d. Pe dispozitivul pe care dorești să instalezi produsul Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.
4. Așteaptă să se finalizeze descărcarea și apoi execută aplicația de instalare.

Validarea instalării

Bitdefender va verifica mai întâi sistemul tău pentru a valida instalarea.

Dacă sistemul tău nu îndeplinește cerințele pentru instalarea Bitdefender, vei fi informat cu privire la aspectele care trebuie îmbunătățite înainte de a putea continua.

Dacă este detectat o soluție antivirus necompatibilă 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 pornești dispozitivul pentru a finaliza dezinstalarea soluțiilor antivirus detectate.

Actualizăm în permanență pachetul de instalare al Bitdefender Total Security.

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

Odată ce instalarea a fost validată, se afișează asistentul de configurare. Urmează pașii pentru a instala Bitdefender Ultimate Small Business Security.

Pasul 1 - Instalarea Bitdefender

Înainte de a începe instalarea, este necesar să îți exprimi acordul cu privire la Contractul de abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Ultimate Small Business Security.

Dacă nu ești de acord cu acești termeni, închide fereastra. Procesul de instalare va fi abandonat și vei ieși din fereastra de instalare.

În cadrul acestui pas se pot efectua două sarcini suplimentare:

- Menține opțiunea **Trimite rapoarte despre produs** activă. Prin permiterea acestei opțiuni, sunt trimise rapoarte către serverele Bitdefender, conținând informații despre modul în care utilizezi produsul. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să îți oferim produse și mai bune pe viitor. Rapoartele nu conțin date confidențiale, cum ar fi numele tău sau adresa IP, și nu vor fi folosite în scopuri comerciale.
- Selectează limba în care dorești să instalezi produsul.

Efectuează clic pe **INSTALARE** pentru a lansa procesul de instalare al produsului tău Bitdefender.

Pasul 2 - Instalare în curs de desfășurare

Așteaptă până când instalarea este finalizată. Sunt afișate informații detaliate cu privire la evoluția instalării.

Pasul 3 - Instalare finalizată

Produsul tău Bitdefender a fost instalat cu succes.

Este afișat rezumatul instalării. Dacă, în timpul instalării, este detectată și dezinstalată o amenințare, poate fi necesară o repornire a sistemului.

Pasul 4 - Analiza dispozitivului

Acum vei fi întrebat dacă dorești să efectuezi o analiză a dispozitivului tău, pentru a te asigura că este în siguranță. În timpul acestui pas, Bitdefender va scana zonele critice ale sistemului. Selectează **Începe analiza dispozitivului** pentru a o iniția.

Poți ascunde interfața de scanare selectând **Rulează scanarea în fundal**. Apoi, alege dacă vrei să fii anunțat când se va încheia scanarea sau nu.

După finalizarea scanării, selectează **Deschide interfața Bitdefender**.

> **Notă**
> În mod alternativ, dacă nu dorești să efectuezi scanarea, poți selecta **Omite**.

Pasul 5 - Primii pași

În fereastra **Primii pași**, poți vizualiza detaliile abonamentului tău activ.

Apasă pe **FINALIZARE** pentru a accesa interfața Bitdefender Ultimate Small Business Security.

Instalare de pe discul de instalare

Pentru a instala Bitdefender de pe discul de instalare, introdu CD-ul în unitatea optică.

În câteva momente se va afișa fereastra de instalare. Urmează instrucțiunile pentru a începe instalarea.

Dacă nu apare ecranul de instalare, utilizează Windows Explorer pentru a parcurge directorul rădăcină al CD-ului și efectuează dublu clic pe fișierul autorun.exe.

În cazul în care viteza ta de internet este slabă sau sistemul tău nu este conectat la internet, efectuează clic pe butonul **Instalare de pe CD/DVD**. În acest caz, va fi instalat produsul Bitdefender disponibil pe disc și o versiune mai nouă se va descărca de pe serverele Bitdefender prin intermediul actualizărilor de produs.

Validarea instalării

Bitdefender va verifica mai întâi sistemul tău pentru a valida instalarea.

Dacă sistemul tău nu îndeplinește cerințele pentru instalarea Bitdefender, vei fi informat cu privire la aspectele care trebuie îmbunătățite înainte de a putea continua.

Dacă este detectat o soluție antivirus necompatibilă 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 pornești dispozitivul pentru a finaliza dezinstalarea soluțiilor antivirus detectate.

Actualizăm în permanență pachetul de instalare al Bitdefender Total Security.

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

Odată ce instalarea a fost validată, se afișează asistentul de configurare. Urmează pașii pentru a instala Bitdefender Ultimate Small Business Security.

Pasul 1 - Instalarea Bitdefender

Înainte de a continua cu instalarea, trebuie să fiți de acord cu Acordul de abonament. Vă rugăm să luați ceva timp pentru a citi Acordul de abonare, deoarece conține termenii și condițiile în care puteți utiliza Bitdefender Ultimate Small Business Security.

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

Două sarcini suplimentare pot fi efectuate la acest pas:

- Păstrează **Trimite rapoarte despre produse** opțiunea activată. Permițând această opțiune, rapoartele care conțin informații despre

modul în care utilizați produsul sunt trimise către serverele Bitdefender. Aceste informații sunt esențiale pentru îmbunătățirea produsului și ne pot ajuta să oferim o experiență mai bună în viitor. Rețineți că aceste rapoarte nu conțin date confidențiale, cum ar fi numele sau adresa dvs. IP și că nu vor fi utilizate în scopuri comerciale.

- Selectați limba în care doriți să instalați produsul.

Clic **INSTALARE** pentru a lansa procesul de instalare a produsului dvs. Bitdefender.

Pasul 2 - Instalare în curs

Așteptați finalizarea instalării. Sunt afișate informații detaliate despre progres.

Pasul 3 - Instalarea s-a încheiat

Este afișat un rezumat al instalării. Dacă orice amenințare activă a fost detectată și eliminată în timpul instalării, poate fi necesară o repornire a sistemului.

Pasul 4 - Analiza dispozitivului

Acum veți fi întrebat dacă doriți să efectuați o analiză a dispozitivului dvs., pentru a vă asigura că este în siguranță. În timpul acestui pas, Bitdefender va scana zonele critice ale sistemului. Clic **Porniți Analiza dispozitivului** pentru a-l iniția.

Puteți ascunde interfața de scanare făcând clic pe **Rulați Scanarea în fundal**. După aceea, alegeți dacă doriți să fiți informat când scanarea este terminată sau nu.

După finalizarea scanării, selectează **Continuă cu Creare cont**.

> **Notă**
> Alternativ, dacă nu doriți să efectuați scanarea, puteți pur și simplu să faceți clic pe **Ocolire**.

Pasul 5 - Contul Bitdefender

După terminarea configurării inițiale vei vedea fereastra Bitdefender Account. Ai nevoie de un cont Bitdefender pentru a activa produsul și pentru a utiliza funcționalitățile online ale acestuia. Pentru mai multe informații, consultă capitolul Bitdefender Central.

Continuă în funcție de situația ta.

- **Vreau să creez un cont Bitdefender**

  1. Introduceți informațiile solicitate în câmpurile corespunzătoare. Informațiile furnizate aici vor rămâne confidențiale. Parola trebuie să aibă o lungime de minimum 8 caractere, să includă cel puțin o cifră sau un simbol și să includă litere mici și mari.
  2. Înainte de a merge mai departe este necesar să îți exprimi acordul cu privire la Condițiile de utilizare. Accesează secțiunea Condiții de utilizare și citește-le cu atenție întrucât conțin termenii și condițiile care îți permit utilizarea Bitdefender.
     Suplimentar, poți accesa și citi Politica de confidențialitate.
  3. Fă clic pe **CREARE CONT**.

     > **Notă**
     > O dată ce contul este creat, poți utiliza adresa de e-mail și parola furnizate pentru a te autentifica în contul tău la https://central.bitdefender.com sau în aplicația Bitdefender Central dacă aceasta este instalată pe unul dintre dispozitivele tale Android sau iOS. Pentru a instala aplicația Bitdefender Central pe Android, este necesar să accesezi Google Play, să cauți Bitdefender Central, iar apoi să apeși pe opțiunea de instalare corespunzătoare. Pentru a instala aplicația Bitdefender Central pe iOS, este necesar să accesezi App Store, să cauți Bitdefender Central, iar apoi să apeși pe opțiunea de instalare corespunzătoare.

- **Am deja un cont Bitdefender**

  1. Fă clic pe **Autentificare**.
  2. Introdu adresa de e-mail în câmpul corespunzător, apoi fă clic pe **MAI DEPARTE**.
  3. Introdu parola și apoi efectuează clic pe **AUTENTIFICARE**.
     Dacă ai uitat parola contului tău sau dacă pur și simplu dorești să o resetezi pe cea existentă deja:
     a. Fă clic pe **Ai uitat parola?**.
     b. Introdu adresa ta de e-mail, apoi selectează opțiunea **ÎNAINTE**.

c. Verificați-vă contul de e-mail, introduceți codul de securitate primit și apoi faceți clic pe **MAI DEPARTE**.
Alternativ, puteți face clic pe **Schimbare parolă** din mesajul e-mail pe care vi l-am trimis.

d. Tastează noua parolă pe care vrei să o setezi, apoi tasteaz-o din nou. Apasă pe **SALVARE**.

> **Notă**
> Dacă ai deja un cont MyBitdefender, îl poți utiliza pentru a te conecta la contul Bitdefender. Dacă ți-ai uitat parola, întâi trebuie să mergi la https://my.bitdefender.com pentru a o reseta. Apoi, utilizează datele de autentificare actualizate pentru a te conecta la contul Bitdefender.

- **Doresc să mă autentific prin intermediul contului de Microsoft, Facebook sau Google**
  Pentru autentificare cu contul tău de Microsoft, Facebook sau Google:
  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 te autentifici de obicei sau datele personale ale prietenilor și contactelor.

Pasul 6 - Activați-vă produsul

> **Notă**
> Această etapă apare dacă ai selectat crearea unui nou cont Bitdefender pe parcursul etapei anterioare sau dacă te-ai autentificat utilizând un cont aferent unui abonament care a expirat.

Este necesară o conexiune activă la internet pentru a finaliza activarea produsului.

Procedează în funcție de situația ta:

- Am un cod de activare
  În acest caz, activează produsul urmând acești pași:

1. Introdu codul de activare în câmpul Am un cod de activare și apoi fă clic pe **CONTINUĂ**.

   Notă
   Iată cum poți găsi codul tău de activare:

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

2. **Vreau să evaluez Bitdefender**
   În acest caz, poți utiliza produsul pentru o perioadă de 30 de zile. Pentru a începe perioada de evaluare, selectează **Nu am un abonament, vreau să încerc gratuit produsul** apoi fă clic pe **CONTINUĂ**.

Pasul 7 - Primii pași

În fereastra **Primii pași**, poți vizualiza detaliile abonamentului tău activ.

Clic **FINALIZAREA** pentru a accesa Bitdefender Ultimate Small Business Security interfata.

3.2. Gestionarea securității

3.2.1. Protecție antivirus

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

- **Scanare la acces** - împiedică pătrunderea amenințărilor noi în sistemul tău. De exemplu, Bitdefender va scana un document word atunci când îl deschizi, pentru a verifica dacă conține amenințări cunoscute, precum și un mesaj e-mail atunci când îl primești.
  Procesul de scanare la accesare asigură protecție în timp real împotriva amenințărilor, fiind o componentă esențială a oricărui program de securitate pentru calculatoare.

> **Important**
> Pentru a preveni infectarea dispozitivului, păstrează activată funcția de **scanare la accesare**.

- **Scanarea la cerere** - permite detectarea și eliminarea amenințărilor 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.

Bitdefender scanează în mod automat orice fișier media amovibil care este conectat la dispozitiv pentru a te asigura că este sigur să îl accesezi. Pentru mai multe informații, consultă capitolul Scanarea automată a suporturilor media amovibile (pagina 34).

Utilizatorii avansați pot configura excepțiile de scanare în cazul în care nu doresc ca anumite fișiere sau tipuri de fișiere să fie scanate. Pentru mai multe informații, consultă capitolul Configurarea excepțiilor de scanare (pagina 36).

Atunci când detectează o amenințare, 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, consultă capitolul Gestionarea fișierelor aflate în carantină (pagina 38).

În cazul în care dispozitivul tău a fost infectat cu amenințări, consultă Eliminarea amenințărilor din sistemul tău (pagina 143). Pentru a te ajuta să îți cureți dispozitivul de amenințările care nu pot fi eliminate din sistemul de operare Windows, Bitdefender îți pune la dispoziție Mediu de salvare (pagina 144). Acesta este un mediu sigur, creat în special pentru eliminarea amenințărilor, care îți permite să pornești dispozitivul în mod independent de Windows. Când dispozitivul funcționează în modul de recuperare, amenințările pentru Windows sunt inactive, ceea ce înseamnă că pot fi eliminate cu ușurință.

Scanare la accesare (protecție în timp real)

Bitdefender oferă protecție în timp real contra unei game extinse de amenințări, scanând toate fișierele și mesajele e-mail accesate.

Activarea sau dezactivarea protecției în timp real

Pentru a activa sau dezactiva protecția în timp real împotriva amenințărilor:

1. Fă clic pe **Protecție** din meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **ANTIVIRUS**, apasă pe **Deschide**.
3. În fereastra **Setări avansate**, activează sau dezactivează **Bitdefender Shield**.
4. Dacă doriți să dezactivați protecția în timp real, se afișează 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 de minute, pentru o oră, permanent sau doar până la repornirea sistemului. Protecția în timp real se va activa automat la expirarea intervalului de timp selectat.

> **Avertizare**
> Aceasta este o problemă majoră de securitate. Îți recomandăm să dezactivezi protecția în timp real pentru cât mai puțin timp posibil. Dacă protecția în timp real este dezactivată, nu vei mai fi protejat împotriva amenințărilor.

Configurarea setărilor avansate 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 avansate de protecție în timp real:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Avansat** poți configura setările scanării după nevoie.

Informații cu privire la opțiunile de scanare

Aceste informații îți pot fi de folos:

- **Scanează numai aplicații.** Poți configura Bitdefender să scaneze doar aplicațiile accesate.
- **Scanează aplicațiile potențial nedorite.** Selectează această opțiune pentru a scana aplicațiile nedorite. O aplicație potențial nedorită (PUA)

sau un program potențial nedorit (PUP) este un software care este, de obicei, integrat într-un software gratuit și care va afișa mesaje pop-up sau va instala o bară de instrumente în browserul implicit. Unele dintre acestea vor schimba pagina principală sau motorul de căutare, altele vor rula o serie de procese în fundal, încetinind calculatorul, sau vor afișa mai multe reclame. Aceste programe pot fi instalate fără consimțământul tău (denumite și adware) sau vor fi incluse implicit în kitul de instalare (susținute prin reclame).

- **Scanează pentru detectarea scripturilor.** Caracteristica Scanează pentru detectarea scripturilor permite Bitdefender să scaneze scripturile powershell și documentele Office care ar putea conține malware bazat pe scripturi.
- **Scanează directoare comune din rețea.** Pentru a accesa în siguranță o rețea de la distanță de pe dispozitivul tău, îți recomandăm să păstrezi activată opțiunea Scanează directoare comune din rețea.
- **Scanează memoria de procesare.** Scanează pentru a detecta activitatea periculoasă în memoria utilizată pentru rularea proceselor.
- **Scanează linie de comandă.** Scanează linia de comandă a aplicațiilor nou lansate pentru a preveni atacurile fileless.
- **Scanează arhive.** Scanarea arhivelor interne este un proces lent și care consumă resurse, prin urmare, nu este recomandat pentru a asigura protecția în timp real. Arhivele care conțin fișiere infectate nu reprezintă o amenințare imediată pentru securitatea sistemului tău. Amenințarea îți poate afecta sistemul doar dacă fișierul infectat este extras din arhivă și executat fără o protecție activată care funcționează în timp real.

  Dacă decizi să utilizezi această opțiune, activeaz-o și apoi trage cursorul pentru a exclude de la scanare arhivele care depășesc o anumită valoare în MB (megaocteți).
- **Scanează sectoarele de boot.** Poți configura Bitdefender să scaneze sectoarele de boot ale hard diskului. Acest sector al hard diskului conține codul necesar pentru a inițiа procesul de boot. În momentul în care o amenințare infectează sectorul de boot, unitatea poate deveni inaccesibilă și este posibil să nu mai poți porni sistemul și accesa datele.

- **Scanează numai fișiere noi și modificate.** Prin scanarea exclusivă a fișierelor noi și a acelor modificate, poți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.
- **Scanează pentru a detecta programe tip keylogger.** Selectează această opțiune pentru a scana sistemul pentru a detecta aplicații de tip keylogger. Aceste aplicații înregistrează ceea ce tastezi pe tastatura ta și trimite rapoarte pe internet către un hacker. Acesta pot afla informații confidențiale din datele furate, precum numerele conturilor bancare și parole și le poate utiliza pentru a obține beneficii personale.
- **Scanare preliminară la încărcarea sistemului.** Selectează opțiunea de **Scanare preliminară la încărcarea sistemului** pentru a scana sistemul la pornire de îndată ce se încarcă toate serviciile importante ale acestuia. Misiunea acestei caracteristici este de a îmbunătăți detecția amenințărilor la pornirea sistemului, precum și timpul de încărcare a sistemului.

Acțiuni aplicate pentru amenințările detectate

Poți configura acțiunile inițiate de protecția în timp real urmând acești pași:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Setări avansate**, derulează în jos până când vezi opțiunea **Acțiuni amenințări**.
4. Configurează setările de scanare după cum este nevoie.

Următoarele acțiuni pot fi inițiate de protecția în timp real în Bitdefender:

Aplică acțiunea adecvată

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

- **Fișiere infectate.** Fișierele detectate ca fiind infectate corespund unei informații privind o amenințare detectată în Baza de date cu informații despre amenințări a Bitdefender. Bitdefender va încerca automat să îndepărteze codul periculos din fișierul infectat și să reconstruiască fișierul inițial. Această operațiune este denumită ca dezinfecție.
  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, consultă capitolul Gestionarea fișierelor aflate în carantină (pagina 38).

> **Important**
> Pentru anumite tipuri de amenințări, dezinfecția nu este posibilă deoarece fișierul detectat este compus în întregime din cod malware. În astfel de situații, fișierul infectat este șters de pe disc.

- **Fișiere suspecte.** Fișierele sunt detectate ca fiind suspecte de către analiza euristică. Fișierele suspecta nu pot fi dezinfectate, întrucât nu există nicio rutină de dezinfecție disponibilă.
- **Arhive care 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.

Mutarea 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, consultă capitolul Gestionarea fișierelor aflate în carantină (pagina 38).

Refuzarea accesului

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

Restaurarea setărilor implicite

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

Pentru a restaura setările implicite pentru protecția în timp real:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.

2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Setări avansate**, derulează în jos până vezi opțiunea **Resetare setări avansate**. Selectează această opțiune pentru a reseta antivirusul la setările prestabilite.

Scanare la cerere

Principalul obiectiv Bitdefender este protejarea dispozitivului tău de amenințări. Aceasta se face nepermițând amenințărilor noi să pătrundă în sistem, prin scanarea mesajelor e-mail și a fișierelor descărcate sau copiate pe dispozitiv.

Există însă riscul ca o amenințare să fi fost în sistem înainte de instalarea Bitdefender. Din acest motiv, este indicat să îți scanezi dispozitivul de amenințări după instalarea Bitdefender. Și este, de asemenea, recomandat să îți scanezi 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. Poți scana dispozitivul oricând dorești prin rularea sarcinilor implicite sau a propriilor sarcini de scanare (sarcini definite de utilizator). Dacă dorești să scanezi anumite locații de pe dispozitivul tău sau să configurezi opțiunile de scanare, poți configura și rula o scanare personalizată.

Scanarea unui fișier sau a unui director pentru detectarea amenințărilor

Se recomandă scanarea fișierelor și directoarelor în orice moment când suspectezi că ar putea fi infectate. Fă clic dreapta pe fișierul sau pe directorul pe care dorești să-l scanezi, indică **Bitdefender** cu mouse-ul și selectează **Scanare cu Bitdefender**. Se va afișa **Asistentul de scanare antivirus** care te va ghida în procesul de scanare. La finalul scanării, ți se va solicita să alegi acțiunile care trebuie implementate asupra fișierelor detectate, dacă este cazul.

Rularea unei scanări rapide

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

Pentru a rula o scanare rapidă:

1. Selectează Protecție din meniul de navigare al interfeței Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În ferestrele **Scanări**, apasă pe butonul **Efectuează scanare** de lângă **Scanare rapidă**.
4. 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.

Executarea unei scanări a sistemului

Sarcina Scanare sistem scanează întregul dispozitiv pentru a depista toate tipurile de amenințări care îi pun în pericol securitatea, cum ar fi programele malware, aplicațiile spion, adware, rootkit-urile și altele.

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

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

- Asigurați-vă că Bitdefender are actualizate bazele de date cu informațiile privind actualizările. Scanarea dispozitivului folosind informații vechi despre amenințări poate împiedica Bitdefender să detecteze noi amenințări descoperite după ultima actualizare efectuată. Pentru mai multe informații, consultă capitolul Cum actualizezi Bitdefender.
- Închide toate programele deschise.

Dacă dorești să scanezi anumite locații de pe dispozitivul tău sau să configurezi opțiunile de scanare, poți configura și rula o scanare personalizată. Pentru mai multe informații, consultă capitolul Configurarea unei scanări personalizate (pagina 27).

Pentru a rula scanarea completă a sistemului:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.

3. În ferestrele **Scanări**, apasă pe butonul **Efectuează scanare** de lângă **Scanare sistem**.
4. La prima rulare a Scanării Sistemului ți se prezintă această caracteristică. Selectează **Ok, am înțeles** pentru a continua.
5. Urmează Expert scanare antivirus pentru a finaliza scanarea. Bitdefender va întreprinde automat acțiunile recomandate pentru fișierele detectate. Dacă rămân amenințări nerezolvate, vi se va solicita să alegeți acțiunile care trebuie întreprinse asupra lor.

Configurarea unei scanări personalizate

În fereastra **Administrare scanări**, poți configura Bitdefender pentru a executa scanări ori de câte ori consideri că dispozitivul tău are nevoie de o verificare pentru depistarea unor potențiale amenințări. Poți opta pentru programarea unei **Scanări de sistem** sau a unei **Scanări rapide**, sau poți crea o sarcină personalizată la alegerea ta.

Pentru a configura în detaliu o nouă scanare personalizată:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În ferestrele **Scanări**, fă clic pe **+Creează scanare**.
4. În câmpul **Nume sarcină**, introdu o denumire pentru scanarea respectivă, apoi selectează locațiile care dorești să fie scanate și fă clic pe **ÎNAINTE**.
5. Configurează următoarele opțiuni generale:
   - **Scanați numai aplicații.** Puteți seta Bitdefender să scaneze numai aplicațiile accesate.
   - **Prioritate scanare sarcină.** Poți alege ce impact ar trebui să aibă un proces de scanare asupra performanței sistemului tău.
     - Automat - Prioritatea procesului de scanare va depinde de activitatea sistemului. Pentru a te asigura că procesul de scanare nu va afecta activitatea sistemului, Bitdefender va decide dacă procesul de scanare trebuie să se execute cu prioritate mare sau mică.
     - Ridicat - Prioritatea procesului de scanare va fi ridicată. Selectând această opțiune, vei permite executarea altor

programe cu o viteză redusă, micșorând perioada de timp necesară pentru finalizarea scanării.

- Redus - Prioritatea procesului de scanare va fi redusă. Selectând această opțiune, vei permite executarea altor programe cu o viteză mai mare, mărind perioada de timp necesară pentru finalizarea scanării.

- **Acțiuni post-scanare.** Alege ce acțiune ar trebuie să implementeze Bitdefender în cazul în care nu sunt identificate amenințări:
  - Afișează fereastra Sumar
  - Închide dispozitivul
  - Închide fereastra Scanare

6. Dacă dorești să configurezi în detaliu opțiunile de scanare, selectează **Afișează opțiuni avansate**. Poți găsi informații referitoare la scanările incluse în listă la sfârșitul acestei secțiuni.
   Apasă pe **Înainte**.
7. Dacă dorești, poți activa opțiunea **Programează sarcina de scanare** și apoi poți alege când ar trebui să pornească sarcina personalizată pe care ai creat-o.
   - La pornirea sistemului
   - Zilnic
   - Lunar
   - Săptămânal

   Dacă selectezi Zilnic, Lunar sau Săptămânal, trage de cursor pentru a seta perioada de timp dorită pentru începerea scanării.
8. Selectează **Salvează** pentru a salva setările și a închide fereastra de configurare.
   Procesul de scanare poate dura ceva timp, în funcție de locațiile ce vor fi scanate. Dacă se vor găsi amenințări în timpul procesului de scanare, ți se va solicita să alegi acțiunile care trebuie întreprinse în cazul fișierelor detectate.

Informații despre opțiunile de scanare

Puteți găsi aceste informații utile:

- Dacă nu sunteți familiarizat cu anumiți termeni, verificați-i în **glosar**. De asemenea, puteți găsi informații utile pe internet.
- **Scanați aplicații potențial nedorite.** Selectați această opțiune pentru a căuta aplicații nedorite. O aplicație potențial nedorită (PUA) sau un program potențial nedorit (PUP) este un software care vine de obicei la pachet cu un software gratuit și va afișa ferestre pop-up sau va instala o bară de instrumente în browserul implicit. Unii dintre ei vor schimba pagina de start sau motorul de căutare, alții vor rula mai multe procese în fundal încetinind PC-ul sau vor afișa numeroase reclame. Aceste programe pot fi instalate fără consimțământul dumneavoastră (numit și adware) sau vor fi incluse implicit în kitul de instalare rapidă (ad-supported).
- **Scanare arhive.** Arhivele care conțin fișiere infectate nu reprezintă o amenințare imediată la adresa securității sistemului tău. Amenințarea îți poate afecta doar dacă fișierul infectat este extras din arhivă și executat fără să fie activată o protecție în timp real. Însă, această opțiune este recomandată pentru a detecta și elimina orice amenințare potențială, chiar dacă nu reprezintă o amenințare imediată.
  Trage cursorul pentru a exclude de la scanare arhivele care depășesc o anumită valoare în MB (megaocteți).

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

- **Scanați numai fișiere noi și modificate.** Scanând numai fișiere noi și modificate, puteți îmbunătăți considerabil capacitatea de răspuns generală a sistemului, cu un compromis minim în materie de securitate.
- **Scanați sectoarele de boot.** Puteți seta Bitdefender să scaneze sectoarele de pornire ale hard diskului. Acest sector al hard diskului conține codul computerului necesar pentru a începe procesul de pornire. Când o amenințare infectează sectorul de pornire, unitatea poate deveni inaccesibilă și este posibil să nu puteți porni sistemul și să vă accesați datele.
- **Scanare memorie.** Selectează această opțiune pentru a scana programele care rulează în memoria sistemului tău.

- **Scanare regiștri.** Selectează această opțiune pentru a scana cheile de regiștri. Windows Registry este o bază de date care stochează setările și opțiunile de configurare ale componentelor sistemului de operare Windows, precum și ale aplicațiilor instalate.
- **Scanare cookie-uri.** Selectează această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe dispozitivul tău.
- **Scanează keylogger-urile.** Selectați această opțiune pentru a vă scana sistemul pentru aplicații keylogger. Keyloggerii înregistrează ceea ce tastați pe tastatură și trimit rapoarte pe internet unei persoane rău intenționate (hacker). Hackerul poate afla informații sensibile din datele furate, cum ar fi numerele de cont bancar și parolele, și le poate folosi pentru a obține beneficii personale.

Asistentul de scanare antivirus

Oricând inițiezi o scanare la cerere (de exemplu, făcând clic dreapta pe un director, indică Bitdefender cu mouse-ul, apoi selectează **Scanare cu Bitdefender**), va apărea asistentul Bitdefender Antivirus Scan. Urmează indicațiile asistentului pentru a efectua procesul de scanare.

> **Notă**
> Dacă asistentul de scanare nu apare, scanarea poate fi configurată să fie efectuată silențios, în fundal. Caută pictograma care arată progresul scanării în **bara de sistem**.

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).

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

Oprirea sau întreruperea scanării. Poți opri scanarea în orice moment dorești apăsând pe **STOP**. Vei fi direcționat direct la ultimul pas al asistentului. Pentru a întrerupe temporar procesul de scanare, trebuie doar să apeși pe **PAUZĂ**. Va trebui să faci clic pe **RELUARE** pentru a relua scanarea.

Arhive protejate cu parolă. Când se detectează o arhivă protejată cu o parolă, în funcție de setările de scanare, este posibil să ți se solicite

parola. Arhivele protejate prin parolă nu pot fi scanate decât dacă introduci parola. Sunt disponibile următoarele opțiuni:

- **Parola.** Dacă vrei ca Bitdefender să scaneze arhiva, selectează această opțiune și introdu parola. Dacă nu cunoști parola, alege una dintre celelalte opțiuni.
- **Nu solicita o parolă și omite acest obiect la scanare.** Selectează această opțiune pentru a omite scanarea acestei arhive.
- **Omite toate elementele protejate cu parolă fără a le scana.** Selectează această opțiune dacă nu vrei să te preocupi de arhivele protejate cu parolă. Bitdefender nu le va putea scana, însă se va păstra o evidență a acestora în jurnalul scanării.

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

Pasul 2 - Selectarea acțiunilor

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

> **Notă**
> Atunci când execuți o scanare rapidă sau o scanare 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 amenințarea 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 aplicată pentru rezolvarea tuturor problemelor găsite, sau puteți alege acțiuni separate pentru fiecare grup de probleme. Una sau mai multe dintre opțiunile următoare pot apărea în meniu:

Aplică acțiunile adecvate

Bitdefender va întreprinde acțiunile recomandate în funcție de tipul de fișier detectat:

- **Fișiere infectate.** Fișierele detectate ca infectate se potrivesc cu o informație de amenințare găsită în Baza de date de informații despre amenințări Bitdefender. Bitdefender va încerca automat să elimine codul rău intenționat din fișierul infectat și să reconstruiască fișierul original. Această operație se numește dezinfecție.

Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a conține infecția. Fișierele puse în carantină nu pot fi executate sau deschise; prin urmare, riscul de a se infecta dispare. Pentru mai multe informații, consultați Gestionarea fișierelor aflate în carantină (pagina 38).

> **Important**
> Pentru anumite tipuri de amenințări, dezinfecția nu este posibilă deoarece fișierul detectat este complet rău intenționat. În astfel de cazuri, fișierul infectat este șters de pe disc.

- **Fisiere suspicioase.** Fișierele sunt detectate ca suspecte de analiza euristică. Fișierele suspecte nu pot fi dezinfectate, deoarece nu este disponibilă nicio rutină de dezinfecție. Aceștia vor fi mutați în carantină pentru a preveni o potențială infecție.
- **Arhive care conțin fișiere infectate.**
  - Arhivele care conțin numai fișiere infectate sunt șterse automat.
  - Dacă o arhivă conține atât fișiere infectate, cât și fișiere curate, Bitdefender va încerca să șteargă fișierele infectate, cu condiția să poată reconstrui arhiva cu fișierele curate. Dacă reconstrucția arhivei nu este posibilă, veți fi informat că nu poate fi luată nicio măsură pentru a evita pierderea fișierelor curate.

Ștergere

Îndepărtează fișierele identificate ca fiind infectate de pe disc.

Dacă într-o arhivă sunt stocate fișiere infectate împreună cu fișiere curate, Bitdefender va 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 efectua 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.

> **Important**
> În majoritatea cazurilor, BitDefender va dezinfecta fișierele infectate detectate sau va izola infecția. 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 amenințărilor în mod manual, consultați Eliminarea amenințărilor din sistemul tău (pagina 143).

Examinarea jurnalelor de scanare

De fiecare dată când efectuezi o scanare, se creează un jurnal de scanare și Bitdefender înregistrează problemele identificate în fereastra 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.

Poți deschide raportul de scanare direct din asistentul de scanare, după ce scanarea a luat sfârșit, apăsând **AFIȘEAZĂ JURNAL**.

Pentru a verifica un jurnal de scanări sau orice infecție detectată ulterior:

1. Clic **Notificări** din meniul de navigare de pe Interfața Bitdefender.
2. În fila **Toate**, selectează notificarea privind ultima scanare.
   Aici poți găsi toate evenimentele de scanare, inclusiv amenințările detectate prin scanarea la accesare, prin scanarea inițiată de utilizator, precum și modificările de stare rezultate de scanările automate.
3. În lista de notificări poți verifica ce operațiuni de scanare au fost realizate recent. Efectuează clic pe o notificare pentru a vizualiza detaliile acesteia.
4. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**.

Scanarea automată a suporturilor media amovibile

Bitdefender detectează automat când conectezi o unitate de stocare amovibilă la dispozitivul tău și o scanează în fundal atunci când este activată opțiunea Scanare automată. Acest lucru este recomandat pentru a preveni pătrunderea amenințărilor pe dispozitivul tău.

Unitățile detectate fac parte din următoarele categorii:

- CD-uri/DVD-uri
- Unitățile de stocare 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.

Cum funcționează?

Când detectează un dispozitiv de stocare amovibil, Bitdefender inițiază scanarea pentru depistarea amenințărilor (cu condiția ca scanarea automată să fie activată pentru acel tip de dispozitiv). Veți fi notificat prin intermediul unei ferestre pop-up că a fost detectat un nou dispozitiv și că aceasta este scanat.

În **bara de sistem** va apărea o pictogramă a procesului de scanare Bitdefender . Poți apăsa pe această pictogramă pentru a deschide fereastra de scanare și pentru a vedea progresul scanării.

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

În majoritatea cazurilor, Bitdefender elimină automat amenințările 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 poate fi aplicată nicio acțiune în cazul fișierelor suspecte detectate pe CD-uri/DVD-uri. De asemenea, în cazul în care nu beneficiați de privilegiile corespunzătoare, nu poate fi aplicată nicio acțiune în cazul fișierelor infectate sau suspecte detectate pe unități mapate de rețea.

Următoarele informații îți pot fi de folos:

- Vă rugăm să acordați atenție maximă atunci când folosiți un CD/DVD infectat cu amenințări, deoarece o amenințare nu poate fi ștearsă de pe CD/DVD (suportul media este de tip read-only). Asigurați-vă că protecția în timp real este activată pentru a preveni răspândirea amenințărilor în cadrul sistemului dvs. Cea 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 amenințările 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 poți gestiona amenințările, consultă Eliminarea amenințărilor din sistemul tău (pagina 143).

Administrarea scanării a fișierelor media amovibile

Pentru a administra scanarea automată a suporturilor media amovibile:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Selectează fereastra **Setări**.

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 malițios) 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.

Pentru cea mai bună protecție, este recomandat să activezi opțiunea **Scanare automată** pentru toate tipurile de dispozitive de stocare amovibile.

Scanare fișier de configurare a gazdelor

Fișierul de configurare a gazdelor vine implicit cu instalarea sistemului de operare și este folosit pentru a mapa numele de gazdă pentru adresele IP de fiecare dată când accesezi o nouă pagină web, te conectezi la FTP sau la alte servere de internet. Este un fișier simplu de tip text, iar programele periculoase îl pot modifica. Utilizatorii avansați știu cum să-l utilizeze pentru a bloca reclamele deranjante, bannerele, cookie-urile terților sau hackerii.

Pentru a configura scanarea fișierului de configurare gazde:

1. Clic **Setări** pe meniul de navigare de pe Interfața Bitdefender.
2. Selectează **Avansat** fila.
3. Activează sau dezactivează opțiunea **Scanare fișier de configurare a gazdelor**.

Configurarea excepțiilor de scanare

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

Poți configura setările astfel încât excepțiile să se aplice doar în cazul scanării la accesare sau al scanării la cerere, sau în cazul ambelor scanări. Obiectele excluse de la scanarea la accesare nu vor fi scanate, indiferent dacă acestea sunt accesate de către tine 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** .

Excluderea fișierelor și directoarelor de la scanare

Pentru a exclude anumite fișiere și directoare de la scanare:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.

2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Setări**, apasă pe **Gestionare excepții**.
4. Apasă pe **+Adaugă o excepție**.
5. Introdu calea directorului pe care vrei să îl excluzi de la scanare în câmpul corespunzător.
   În mod alternativ, poți naviga către director făcând clic pe butonul de navigare din partea dreaptă a interfeței, selectându-l și făcând clic pe **OK**.
6. Activează butonul de lângă caracteristica de protecție care nu trebuie să scaneze directorul. Există trei opțiuni:
   - Antivirus
   - Online Threat Prevention
   - Advanced Threat Defense
7. Faceți clic pe **Salvează** pentru a salva modificările și închide fereastra.

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 dispozitiv. 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**
> Acționează cu grijă atunci când setezi excepții de scanare pentru extensiile de fișiere deoarece asemenea excepții pot face dispozitivul vulnerabil în fața amenințărilor.

Pentru a exclude extensii de fișiere de la scanare:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În **Setări** fereastra, faceți clic **Gestionați excepțiile**.
4. Clic **+ Adăugați o excepție**.
5. Introdu extensiile care dorești să fie excluse de la scanare cu un punct înaintea lor, separându-le prin punct și virgulă (;).

txt;avi;jpg

6. Activează butonul de lângă caracteristica de protecție care nu trebuie să scaneze extensia.
7. Fă clic pe **Salvare**.

Administrarea excepțiilor de scanare

Dacă excepțiile de scanare configurate nu mai sunt necesare, se recomandă să le ștergi sau să dezactivezi excepțiile de scanare.

Pentru a administra excepțiile de scanare:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Setări**, apasă pe **Gestionare excepții**. Se afișează o listă cu toate excepțiile.
4. Pentru a șterge sau edita excepțiile de scanare, selectează unul dintre butoanele disponibile. Procedați astfel:
   - Pentru a șterge o înregistrare din listă, fă clic pe butonul din dreptul său.
   - Pentru a edita o înregistrare din tabel, selectează butonul **Editare** de lângă aceasta. Se afișează o nouă fereastră unde poți schimba extensia sau calea care va fi exclusă, precum și caracteristica de securitate de la care acestea să fie excluse, după caz. Efectuează modificările necesare, apoi dă clic pe **MODIFICĂ**.

Gestionarea fișierelor aflate în carantină

Bitdefender izolează fișierele infectate cu amenințări ce nu pot fi dezinfectate, precum și fișierele suspecte într-o zonă sigură numită carantină. Atunci când sunt în carantină, amenințările sunt inofensive, pentru că nu pot fi executate sau citite.

În plus, Bitdefender scanează fișierele din carantină după fiecare actualizare a bazei de date cu amenințări. Fișierele curățate sunt mutate automat în locația lor originală.

Pentru a verifica și gestiona fișierele din carantină:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.

2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Mergi la fereastra **Setări**.
   Aici poți vizualiza denumirile fișierelor în carantină, localizarea lor originală și denumirea amenințărilor detectate.
4. Fișierele aflate în carantină sunt gestionat în mod automat de Bitdefender, în funcție de setările implicite pentru carantină.
   Deși nu este recomandat, poți modifica setările de carantină în funcție de preferințele tale efectuând clic pe **Vizualizare setări**.
   Efectuează clic pe comutatoare pentru a activa sau dezactiva:
   Scanează din nou carantina după actualizarea informațiilor despre amenințări
   Mențineți activată această opțiune pentru a scana în mod automat fișiere aflate în carantină după fiecare actualizare a bazei de date cu informații privind amenințările. Fișierele curățate sunt mutate automat în locația lor originală.
   Ștergere conținutul mai vechi de 30 de zile
   Fișirele aflate în carantină mai vechi de 30 de zile sunt șterse automat.
   Creează excepții pentru fișierele restabilite
   Fișierele pe care le restabilești din carantină sunt mutate înapoi în locația lor inițială fără a fi reparate și sunt automat excluse de la scanările următoare.
5. 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**.

3.2.2. Apărare avansată împotriva amenințărilor

Bitdefender Advanced Threat Defense este o tehnologie inovatoare de detecție proactivă, care folosește metode euristice avansate pentru a detecta ransomware și alte amenințări noi potențiale în timp real.

Advanced Threat Defense monitorizează continuu aplicațiile care rulează pe dispozitivul tău, căutând amenințări. Fiecare dintre aceste acțiuni are un anumit punctaj iar punctajul global este calculat pentru fiecare proces.

Ca o măsură de siguranță, vei fi anunțat de fiecare dată când se detectează și se blochează amenințări și procese potențial periculoase.

Activarea sau dezactivarea funcției Advanced Threat Defense

Pentru a activa sau dezactiva funcția Advanced Threat Defense

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **ADVANCED THREAT DEFENSE**, fă clic pe **DESCHIDE**.
3. Accesează fereastra **Setări** și selectează butonul de lângă **Bitdefender Advanced Threat Defense**.

> **Notă**
> Pentru a-ți menține sistemul protejat de ransomware și toate celelalte amenințări, îți recomandăm să dezactivezi funcția Advanced Threat Defense cât mai puțin timp posibil.

Verificarea atacurilor malware detectate

Ori de câte ori sunt detectate amenințări sau procese potențial dăunătoare, Bitdefender le va bloca pentru a preveni infectarea dispozitivului cu ransomware sau cu alte programe malware. Poți verifica în orice moment lista atacurilor malware detectate urmând acești pași:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Apărare avansată împotriva amenințărilor** panou, faceți clic **Deschis**.
3. Mergi la fereastra **Threat Defense**.
   Sunt afișate atacurile detectate în ultimele 90 de zile. Pentru a afla detalii despre tipul de ransomware detectat, calea procesului periculos, sau dacă dezinfectarea a fost efectuată cu succes, efectuează clic pe acesta.

Adăugarea proceselor în lista de excepții

Poți configura regulile de excludere pentru aplicațiile sigure astfel încât funcția Advanced Threat Defense să nu le blocheze dacă întreprind acțiuni ce pot părea amenințătoare.

Pentru a începe adăugarea proceselor în lista de excepții a funcției Advanced Threat Defense:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Apărare avansată împotriva amenințărilor** panou, faceți clic **Deschis**.
3. În **Setări** fereastra, faceți clic **Gestionați excepțiile**.
4. Clic **+ Adăugați o excepție**.

5. Introduceți calea folderului pe care doriți să-l faceți, cu excepția scanării, în câmpul corespunzător.
   În mod alternativ, poți naviga către fișierul executabil făcând clic pe butonul de navigare din partea dreaptă a interfeței, selectându-l și făcând clic pe **OK**.
6. Activează butonul de lângă **Advanced Threat Defense**.
7. Clic **Salvați**.

Detecție exploit-uri

Una dintre metodele folosite de hackeri pentru a pătrunde în sisteme este de a profita de anumite erori sau vulnerabilități prezente în software-ul (aplicații sau plugin-uri) și hardware-ul computerelor. Pentru a te asigura că dispozitivul tău este protejat de astfel de atacuri, care în mod normal se răspândesc foarte rapid, Bitdefender utilizează cele mai noi tehnologii anti-exploit-uri.

Activarea sau dezactivarea funcției de detecție exploit-uri

Pentru a activa sau dezactiva funcția de detecție exploit-uri:

- Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
- În **Apărare avansată împotriva amenințărilor** panou, faceți clic **Deschis**.
- Accesează fereastra **Setări** și selectează butonul de lângă **Detecție exploit-uri** pentru a activa sau dezactiva caracteristica.

> **Notă**
> Opțiunea Detecție exploit-uri este activată în mod implicit.

3.2.3. Prevenirea amenințărilor online

Bitdefender Online Threat Prevention asigură o experiență de navigare în siguranță, alertându-te cu privire la posibilele pagini web periculoase.

Bitdefender oferă funcția de prevenire în timp real a amenințărilor pentru:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox

- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Pentru a configura setările Online Threat Prevention:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **ONLINE THREAT PREVENTION**, fă clic pe **Setări**.

În secțiunile **Protecție web**, selectează butoanele pentru activare sau dezactivare:

- Funcția de prevenire a atacurilor web blochează amenințările care vin de pe internet, inclusiv descărcările neintenționate.
- 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 îți recomandăm să vizitezi această pagină web.

  Această pagină poate avea conținut periculos. Procedează cu precauție dacă decizi să o vizitezi.

  Aceasta este o pagină 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

- Scanare web criptată.

Atacurile mai sofisticate pot folosi trafic de web securizat pentru a induce în eroare victimele. Prin urmare, îți recomandăm să păstrezi activată opțiunea Scanare web criptată.

- Protecție antifraudă.
- Protecție antiphishing.

Derulează și vei ajunge la secțiunea **Network threat prevention**. Aici vei găsi opțiunea **Network threat prevention**. Pentru a îți păstra dispozitivul protejat împotriva atacurilor programelor periculoase (cum ar fi ransomware) prin exploatarea vulnerabilităților, păstrează activă această opțiune.

Poți crea o listă de site-uri, domenii și adrese IP care nu vor fi scanate de motoarele contra amenințărilor, tentativelor de phishing și antifraudă Bitdefender. Lista trebuie să conțină numai site-uri web, domenii și adrese IP în care aveți încredere deplină.

Pentru a configura și administra site-urile web, domeniile și adresele IP folosind funcția Online Threat Prevention pusă la dispoziție de Bitdefender:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **PREVENIREA AMENINȚĂRILOR ONLINE** panou, faceți clic **Setări**.
3. Apasă pe **Gestionare excepții**.
4. Clic **+ Adăugați o excepție**.
5. Introdu în câmpul corespunzător denumirea site-ului web, numele domeniului sau adresa IP pe care dorești să o adaugi la excepții.
6. Activează butonul de lângă **Online Threat Prevention**.
7. Pentru a elimina o intrare din listă, faceți clic pe butonul de lângă el. Clic **Salvați** pentru a salva modificările și a închide fereastra.

Alertele Bitdefender din browser

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

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

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

- Părăsește site-ul web respectiv dând clic pe **REVENIRE LA O PAGINĂ SIGURĂ**.
- Accesați site-ul web, în ciuda avertismentului, făcând clic pe **Înțeleg riscurile și doresc să accesez această pagină**.
- Dacă ești sigur că pagina web detectată este sigură, selectează **TRIMITE** pentru a o adăuga în lista de excepții. Îți recomandăm să adaugi numai pagini web în care ai deplină încredere.

3.2.4. Protecție pentru e-mail

E-mailul tău este o parte importantă a vieții tale digitale și, având în vedere multiplele sale aplicații în viața reală, a devenit un vector de atac preferat pentru actorii răi și una dintre preocupările principale de securitate cibernetică ale utilizatorului obișnuit.

Protecție pentru e-mail este o funcție de securitate care vă permite să scanați și să identificați conținut potențial periculos din e-mailurile primite în căsuța dvs. de e-mail. Această caracteristică este un pachet cu o varietate de tehnologii reunite sub același modul de protecție, cum ar fi software anti-phishing, antimalware, antispam, antifraudă și anti-escrocherie.

Prin crearea unei conexiuni directe între Bitdefender și furnizorul dvs. de servicii de e-mail, permiteți antivirusului să vă scaneze direct e-mailurile și să eliminați limitările generate de utilizarea diferitelor dispozitive sau clienți de e-mail.

> **Notă**
> Puteți proteja până la 5 conturi de e-mail diferite.

Configurarea contului dvs

Această caracteristică este integrată perfect în interfața cu utilizatorul. Pentru a începe să utilizați Protecția e-mailului:

1. In panoul **Protecție**, faceți clic pe **Deschis** în cardul **Protecție pentru e-mail**.
2. Alegeți furnizorul dvs. de e-mail pentru contul de e-mail pe care doriți să îl protejați.

> **Notă**
> Protecția pentru e-mail este disponibilă în prezent pentru conturile Google, conturile Outlook și în curând va fi disponibilă și pentru Yahoo Mail.

3. Faceți clic pe **Conectare**.
   Operația va continua apoi în browser.
4. Introduceți adresa dvs. de e-mail și faceți clic pe **Inainte**.
5. Pentru a continua, introduceți parola și faceți clic pe **Inainte**.
6. Verificați permisiunile solicitate pe ecran și permiteți Bitdefender să vă protejeze contul de e-mail.

Contul dvs. de e-mail este acum protejat și toate noile e-mailuri primite vor fi scanate împotriva amenințărilor.

> **Notă**
> Fiecare e-mail scanat va fi marcat cu o etichetă pentru a indica nivelurile sale de siguranță.

Tabloul de Bord

Tabloul de bord va afișa e-mailurile dvs. protejate sub care veți găsi:

- data de configurare (data la care contul a fost configurat pentru Protecție pentru e-mail)
- stare (activ sau inactiv)
- numărul de e-mailuri filtrate în ultimele 30 de zile.
  Aici veți vedea o diagramă care arată numărul de e-mailuri sigure și e-mailuri periculoase primite.

Pentru a adăuga mai multe conturi de e-mail faceți clic pe **Adăugați un alt cont** și parcurgeți procesul de configurare de mai sus pentru fiecare dintre ele.

Pentru a întrerupe scanarea sau a elimina un cont din această caracteristică faceți clic pe cele trei puncte de lângă contul în cauză și faceți clic pe **Gestionați contul**.

3.2.5. 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, consultă capitolul Detalii privind modulul Antispam (pagina 46).

Protecția Bitdefender Antispam este disponibilă doar pentru clienții de e-mail configurați să primească mesaje e-mail prin protocolul POP3. POP3 este unul dintre cele mai utilizate protocoale pentru descărcarea mesajelor e-mail de la un server de corespondență.

> **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 câmpul subiectului. Bitdefender mută automat mesajele într-un anumit director, după cum urmează:

- În Microsoft Outlook, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Obiecte șterse**. Directorul **Spam** este creat atunci când un e-mail este etichetat ca spam.
- În Mozilla Thunderbird, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Trash**. Directorul **Spam** este creat atunci când un e-mail este etichetat ca spam.

Dacă utilizezi alți clienți de mail, trebuie să creezi o regulă pentru mutarea mesajelor e-mail marcate ca [spam] de Bitdefender într-un director special de carantină. Dacă elementele șterse sau directoarele Trash sunt șterse, și directorul Spam va fi șters. Însă, de îndată ce un e-mail este etichetat ca spam, va fi creat un nou director Spam.

Detalii privind modulul Antispam

Caracteristica antispam are următoarele funcții și setări:

Filtrele Antispam

Motorul antispam de la Bitdefender include protecție cloud și diverse alte filtre care îți protejează Inboxul împotriva mesajelor de tip SPAM, cum ar fi **Lista de prieteni**, **Lista de spammeri** și **Filtrul de caractere**.

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**. Bitdefender nu 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.

Funcționarea Antispam

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

Fiecare e-mail primit pe internet este întâi verificat prin aplicarea filtrului **Lista de prieteni**/**Lista de spammeri**. Dacă adresa expeditorului se regăsește în **lista de prieteni** mesajul este mutat direct în **Inboxul** tău.

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**.

Notă
Dacă e-mailul este marcat ca având CONȚINUT SEXUAL EXPLICIT în câmpul subiectului, Bitdefender îl va considera SPAM.

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 / 2013 / 2016 / 2019
- Mozilla Thunderbird 14 și versiuni ulterioare

Activarea sau dezactivarea protecției antispam

Protecția antispam este activată implicit.

Pentru a activa sau dezactiva caracteristica Antispam:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **ANTISPAM**, activează sau dezactivează butonul.

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 cel mai frecvent utilizați clienți de mail, printr-o bara de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de mail admiși, consultați Clienți și protocoale de e-mail compatibile (pagina 48).

Fiecare buton al barei de comenzi este explicat mai jos:

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

Este spam - indică faptul că e-mailul selectat este spam. E-mailul va fi mutat imediat în directorul {9}Spam{10}. Dacă serviciile antispam în cloud sunt activate, mesajul este trimis la Bitdefender Cloud pentru a fi analizat.

Nu este spam - indică faptul că e-mailul selectat nu este spam și Bitdefender nu ar fi trebuit să-l marcheze astfel. E-mailul va fi mutat din directorul **Spam** în directorul **Inbox**. Dacă serviciile antispam în cloud sunt activate, mesajul este trimis la Bitdefender Cloud pentru a fi analizat.

> **Important**
>
> Butonul **Nu este spam** devine activ atunci când selectezi un mesaj marcat ca SPAM de către Bitdefender (în mod normal, aceste mesaje se află în directorul **Spam**).

Adăugare spammer - adaugă expeditorul e-mailului selectat pe lista de spammeri. Pentru a confirma, este posibil să trebuiască să faci clic pe **OK**. Mesajele e-mail primite de la adrese de pe lista spammerilor sunt marcate automat ca [spam].

Adăugare prieten - adaugă expeditorul e-mailului selectat pe lista de prieteni. Pentru a confirma, este posibil să trebuiască să faci clic pe **OK**. Vei primi întotdeauna mesajele e-mail de la această adresă indiferent ce conțin.

Spammeri - deschide **lista de spammeri** care conține toate adresele de e-mail de la care nu dorești să primești mesaje, indiferent de conținutul lor. Pentru mai multe informații, consultă Configurarea listei de spammeri (pagina 52).

Prieteni - deschide **lista de prieteni** care conține toate adresele de e-mail de la care dorești să primești mesaje e-mail întotdeauna, indiferent de conținutul lor. Pentru mai multe informații, consultă Configurarea listei de prieteni (pagina 51).

Indicarea erorilor de detecție

Dacă folosești un client de e-mail compatibil, poți corecta cu ușurință filtrul antispam (indicând ce mesaje e-mail nu ar trebui marcate ca fiind de tip [spam]). Astfel, vei îmbunătăți eficiența filtrului antispam. Urmează acești pași:

1. Deschide clientul tău de mail.
2. Mergi în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectează mesajele legitime pe care Bitdefender le-a marcat incorect ca [spam].

4. Fă clic pe butonul **Adăugare prieten** din bara de instrumente Bitdefender antispam pentru a adăuga expeditorul pe lista de prieteni. Pentru a confirma, este posibil să trebuiască să faci clic pe **OK**. Vei primi întotdeauna mesajele e-mail de la această adresă indiferent ce conțin.

5. Efectuează 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.

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 de e-mail.
2. Mergi la directorul Inbox.
3. Selectează mesajele spam nedetectate.
4. Fă clic pe butonul **Este spam** din bara de instrumente Bitdefender antispam (situată în mod normal în partea superioară a ferestrei clientului de e-mail). Mesajele vor fi marcate imediat ca fiind de tip [spam] și mutate în directorul de e-mail-uri nedorite (junk).

Configurarea setărilor barei de instrumente

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

Aici ai la dispoziție următoarele opțiuni:

- **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.
- Poți alege dacă se afișează sau nu ferestrele de confirmare când faci clic pe butoanele **Adăugare spammer** și **Adăugare 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.

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 {1**lista de prieteni** va fi trimis automat în directorul Inbox, fără a mai fi procesat.

Pentru a configura și administra lista de prieteni:

- Dacă utilizezi Microsoft Outlook sau Thunderbird, apasă pe butonul Prieteni din **bara de instrumente Bitdefender antispam**.
- Alternativ:
  1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
  2. În secțiunea **ANTISPAM**, fă clic pe **Setări**.
  3. Mergi la fereastra **Administrare prieteni**.

Pentru a adăuga o adresă de e-mail, selectează opțiunea **Adresă e-mail**, introduc adresa și apoi apasă pe **ADĂUGARE**. Sintaxă: name@domain.com.

Pentru a adăuga toate adresele de e-mail dintr-un anumit domeniu, selectează opțiunea **Nume domeniu**, introdu numele domeniului și efectuează clic pe **Adăugare**.

- @domain.com și domain.com - toate mesajele primite de la domain.com vor ajunge în directorul **Inbox** indiferent de conținut;
- 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. 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 obiect din listă, apară pe butonul corespunzător din dreptul obiectului. Pentru a șterge toate elementele din listă, apasă **Ștergere listă**.

Poți salva Lista de prieteni într-un fișier, astfel încât s-o poți folosi pe un alt dispozitiv 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 memorată anterior, selectează **Încarcă** și deschide fișierul corespunzător .bwl. Pentru a reseta conținutul listei curente atunci când încarci o listă salvată anterior, bifează caseta de lângă **Suprascrie lista curentă**.

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 utilizezi Microsoft Outlook sau Thunderbird, apasă pe butonul **Spammeri** din **bara de instrumente Bitdefender antispam** integrată în clientul tău de e-mail.
- Alternativ:

  1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
  2. În **ANTI SPAM** panou, faceți clic **Setări**.
  3. Mergi la fereastra **Administrare spammeri**.

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

Pentru a adăuga toate adresele de e-mail dintr-un anumit domeniu, selectați **Numele domeniului** opțiunea, introduceți numele domeniului, apoi faceți clic **ADĂUGA**. Sintaxă:

- @domain.comand domain.com - toate mesajele e-mail primite de la domain.com vor ajunge în **Inboxul** tău indiferent de conținutul lor;
- domeniu - toate mesajele de e-mail primite de la domeniu (indiferent de sufixele de domeniu) vor fi etichetate ca SPAM;
- com - a- toate mesajele primite având sufixul domeniului com vor fi etichetate ca SPAM.

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

> **Avertizare**
> Nu adăuga domeniile serviciilor de e-mail legitime, furnizate prin web (precum Yahoo, Gmail, Hotmail sau altele) în lista de spammeri. Dacă faci asta, mesajele e-mail primite de la orice utilizator înregistrat al unui astfel de serviciu vor fi detectate ca spam. De exemplu, dacă adaugi **yahoo.com** în lista de spammer, toate mesajele e-mail trimise de la adrese **yahoo.com** vor fi marcate ca [spam].

Pentru a șterge un articol din listă, faceți clic pe butonul corespunzător butonul de lângă el. Pentru a șterge toate intrările din listă, faceți clic **Listă clară**.

Poți salva Lista de prieteni într-un fișier, astfel încât s-o poți folosi pe un alt dispozitiv 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 memorată anterior, efectuează clic pe **ÎNCARCĂ** și deschide fișierul corespunzător .bwl. Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior, selectați Suprascrie lista curentă.

Se configurează filtrele locale antispam

Conform descrierii de la Detalii privind modulul Antispam (pagina 46), 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:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTI SPAM** panou, faceți clic **Setări**.
3. Mergi la fereastra **Setări** și selectează butoanele corespunzătoare de activare sau dezactivare.

Dacă utilizezi Microsoft Outlook sau Thunderbird, poți configura filtrele locale antispam direct din clientul de e-mail. Apasă pe butonul **Setări** din bara de instrumente Bitdefender antispam (situată, de obicei, în partea de sus a ferestrei clientului de e-mail) și apoi deschide fila **Filtre antispam**.

Configurarea setărilor cloud

Funcția de detecție cloud folosește serviciile Bitdefender Cloud pentru a vă oferi protecție antispam eficientă și constant actualizată.

Protecția cloud funcționează cât timp caracteristica Bitdefender Antispam este activă.

Poți trimite mostre de mesaje e-mail legitime și de tip spam către Bitdefender Cloud în cazul în care identifici erori de detecție sau mesaje e-mail de tip spam nedetectate. Acest lucru contribuie la îmbunătățirea ratei de detecție a Bitdefender antispam.

Configurează trimiterea mostrelor de e-mail către Bitdefender Cloud selectând opțiunile dorite și urmărind pașii de mai jos:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTI SPAM** panou, faceți clic **Setări**.
3. Du-te la **Setări** fereastra și faceți clic pe comutatoarele de pornire sau dezactivare corespunzătoare.

Dacă utilizezi Microsoft Outlook sau Thunderbird, poți configura funcția de detecție cloud direct din clientul de e-mail. Apasă pe butonul **Setări** din

bara de instrumente Bitdefender antispam (situată, de obicei, în partea de sus a ferestrei clientului de e-mail) și apoi deschide fila **Setări cloud**.

3.2.6. Firewall

Reține
Modulul Firewall din cadrul Bitdefender Ultimate Small Business Security va fi dezactivat în mod implicit. Va trebui să îl activezi manual.

Dacă **Windows Defender Firewall** este activat în timpul acestei proceduri, ți se va solicita să îl dezactivezi mai întâi.

Firewall-ul îți protejează dispozitivul împotriva încercărilor de conectare neautorizată la intrare și la ieșire, atât în rețelele locale, cât și pe internet. Este asemănător unui paznic care păzește o intrare - urmărește încercările de conectare și decide pe care să le permită și pe care să le blocheze.

Firewall-ul Bitdefender utilizează un set de reguli pentru a filtra datele transmise către și de la sistemul tău.

În condiții normale, Bitdefender creează automat o regulă ori de câte ori o aplicație încearcă să acceseze internetul. De asemenea, poți adăuga sau edita manual reguli pentru aplicații.

Ca măsură de siguranță, vei fi notificat de fiecare dată când se blochează accesul la internet pentru o aplicație potențial periculoasă.

Bitdefender atribuie automat un tip de rețea fiecărei conexiuni de rețea pe care o detectează. 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 poți edita setările de rețea, acceseazăAdministrarea setărilor de conectare (pagina 58).

Activarea sau dezactivarea protecției firewall

Pentru a activa sau dezactiva protecția firewall:

1. Fă clic pe **Securitate** în meniul de navigare din interfața Bitdefender.
2. În panoul **FIREWALL**, activează sau dezactivează butonul aferent.

Atenție
Deoarece dezactivarea firewall-ului îți expune dispozitivul la conexiuni neautorizate, ar trebui să fie doar o măsură temporară. Reactivează firewall-ul cât mai repede posibil.

Administrarea regulilor pentru aplicații

Pentru a vizualiza și a administra regulile pentru firewall, ce controlează accesul aplicațiilor la resursele rețelei și la internet:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **FIREWALL**, fă clic pe **Setări**.
3. Mergi la fereastra **Acces aplicație**.

Poți vedea cele mai noi programe (procese) care au trecut prin Bitdefender Firewall și prin rețeaua de internet la care ești conectat. Pentru a vedea regulile create pentru o anumită aplicație, fă clic pe aplicație, apoi pe linkul **Vizualizare reguli aplicație**. Se deschide fereastra **Reguli**.

Pentru fiecare regulă sunt afișate următoarele informații:

- **REȚEA** - procesul și tipurile de adaptoare de rețea (Acasă/Birou, Public sau Toate) pentru care se aplică regula. Regulile sunt create automat pentru a filtra accesul la rețea sau internet prin oricare adaptor. În mod implicit, regula se aplică oricărei rețele. 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. În mod implicit, regula se aplică oricărui protocol.
- **TRAFIC** - regula se aplică în ambele direcții, atât traficului de intrare și celui de ieșire.
- **PORTURI** - protocolul de PORTURI căruia i se aplică regula. În mod implicit, regula se aplică tuturor porturilor.
- **IP** - protocolul de internet (IP) căruia i se aplică regula. În mod implicit, regula se aplică tuturor adreselor IP.
- **ACCES** - dacă accesul aplicației la rețea sau la internet este permis sau respins în condițiile precizate.

Pentru a edita sau șterge regulile unei anumite aplicații, apasă pe pictograma ⋯.

- **Modificare regulă** - deschide o fereastră în care puteți modifica regula curentă.

- **Ștergere regulă** - poți alege să ștergi setul de reguli curent pentru aplicația selectată.

Adăugare reguli pentru aplicații

Pentru adăugarea unei reguli pentru aplicație:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **FIREWALL** panou, faceți clic **Setări**.
3. În fereastra **Reguli**, apasă pe **Adăugare regulă**.

Aici poți aplica următoarele modificări:

- **Aplică această regulă tuturor aplicațiilor.** Activează acest buton pentru a aplica regula creată tuturor aplicațiilor.
- **Calea programului.** Apasă pe **RĂSFOIRE** și selectează aplicația căreia i se aplică regula.
- **Permisiune.** Selectează una dintre permisiunile disponibile:

Drept de acces	Descriere
Permite	Aplicației specificate îi va fi permis accesul la rețea / internet în condițiile specificate.
Respinge	Aplicației specificate îi va fi refuzat accesul la rețea / internet în condițiile specificate.

- **Tip rețea.** Selectează tipul de rețea căreia i se aplică regula. Poți schimba tipul deschizând meniul vertical **Tip rețea** și selectând unul dintre tipurile disponibile în listă.

Tip rețea	Descriere
Orice rețea	Permite tot traficul dintre dispozitivul tău și alte dispozitive indiferent de tipul rețelei.
Acasă/Birou	Permite tot traficul către și de la dispozitivele din rețeaua locală.
Publică	Tot traficul este filtrat.

- **Protocol.** Selectează 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 dorești ca regula să fie aplicată pentru ICMP, selectează **ICMP**.
- Dacă dorești ca regula să fie aplicată pentru IGMP, selectează **IGMP**.
- Dacă dorești ca regula să fie aplicată pentru GRE, selectează **GRE**.
- Dacă dorești ca o regulă să se aplice unui anumit protocol, introdu în câmpul gol numărul alocat protocolului pe care dorești să-l filtrezi.

> **Notă**
> Numerele de protocol IP sunt atribuite de Autoritatea de atribuire a numerelor de internet (IANA). Poți găsi lista completă de numere de protocol IP atribuite le adresa http://www.iana.org/assignments/protocol-numbers.

- **Direcție.** Selectează din meniu direcția traficului căreia i se aplică regula.

Direcție	Descriere
De ieșire	Regula nu se va aplica decât pentru traficul la ieșire.
De intrare	Regula nu se aplica decât pentru traficul la intrare.
Ambele	Regula se va aplica în ambele direcții.

Selectează butonul **Setări avansate** din partea inferioară a ferestrei pentru a personaliza următoarele setări:

- **Adresă locală personalizată.** Precizează adresa IP și portul local cărora li se aplică regula.
- **Adresa personalizată la distanță.** Specificați adresa IP și portul de la distanță cărora li se aplică regula.

Pentru a îndepărta setul actual de reguli și a restabili regulile implicite, fă clic pe **Resetare reguli** din fereastra **Reguli**.

Administrarea setărilor de conectare

Indiferent că te conectezi la internet printr-un adaptor Wi-Fi sau printr-un adaptor Ethernet, poți configura setările care dorești să fie aplicate pentru o navigare sigură. Opțiunile disponibile sunt următoarele:

- **Dinamic** – tipul rețelei va fi setat automat în funcție de profilul rețelei conectate, Acasă/Birou sau Public. Atunci când se întâmplă acest lucru, se vor aplica numai regulile de Firewall valabile pentru tipul de rețea respectiv sau cele definite pentru a se aplica tuturor tipurilor de rețea.
- **Acasă/Birou** – tipul de rețea va fi întotdeauna Acasă/Birou, indiferent de profilul rețelei conectate. Atunci când se întâmplă acest lucru, se vor aplica numai regulile de Firewall pentru modul Acasă/Birou sau cele definite pentru a se aplica tuturor tipurilor de rețea.
- **Public** - tipul de rețea va fi întotdeauna Public, indiferent de profilul rețelei conectate. Atunci când se întâmplă acest lucru, se vor aplica numai regulile de Firewall pentru modul Public sau cele definite pentru a se aplica tuturor tipurilor de rețea.

Pentru a configura adaptoarele de rețea:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **FIREWALL** panou, faceți clic **Setări**.
3. Selectează fereastra **Adaptoare rețea**.
4. Selectează setările care dorești să fie aplicate atunci când te conectezi la următoarele adaptoare:
   - Wi-Fi
   - Ethernet

Configurarea setărilor avansate

Pentru a configura setări avansate de firewall:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În **FIREWALL** panou, faceți clic **Setări**.
3. Selectează **Setări** fereastră.

Pot fi configurate următoarele caracteristici:

- **Protecția scanării porturilor** - detectează și blochează tentativele de a afla ce porturi sunt deschise.
  Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe dispozitivul tău. Dacă este detectat un port vulnerabil, aceștia pot pătrunde în dispozitivul tău.

- **Mod alertă** - alertele sunt afișate de fiecare dată când o aplicație încearcă să se conecteze la internet. Selectează **Permite** sau **Blocare**. Când modul Alertă este activat, caracteristica **Profiluri** este dezactivată automat. Modul alertă poate fi utilizat concomitent cu **Modul baterie**.
- **Permite accesul la rețeaua de domeniu** - permiteți sau refuză accesul la resurse și locații partajate definite de controllerele de domeniu.
- **Mod ascuns** - dacă poți fi detectat de alte dispozitive. Efectuează clic pe **Modificare setări mod ascuns** pentru a selecta când dispozitivul tău ar trebui și când nu ar trebui să fie vizibil pentru alte dispozitive.
- **Comportament implicit al aplicației** - permite Bitdefender să aplice setările automate pentru aplicațiile fără reguli definite. Efectuează clic pe **Modificare reguli implicite** pentru a selecta dacă setările automate trebuie aplicate sau nu.
  - Automat - accesul aplicațiilor va fi permis sau blocat pe baza setărilor automate de Firewall și a regulilor utilizatorului.
  - Permite - se va permite în mod automat accesul aplicațiilor care nu au definită nicio regulă de Firewall.
  - Blochează - se va bloca în mod automat accesul aplicațiilor care nu au definită nicio regulă de Firewall.

3.2.7. Vulnerabilități

Un pas important în protejarea dispozitivului tău împotriva acțiunilor și aplicațiilor periculoase este de a menține actualizat sistemul de operare și aplicațiile pe care le utilizezi în mod regulat. Mai mult, pentru a împiedica accesul fizic neautorizat la dispozitivul tău, este necesară configurarea de parole puternice (parole ce nu pot fi ghicite cu ușurință) pentru fiecare cont de utilizator Windows, precum și pentru rețelele Wi-Fi la care te conectezi.

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

- Puteți scana sistemul pentru a identifica vulnerabilitățile acestuia și le puteți remedia pas cu pas folosind opțiunea **Scanare vulnerabilitate**.
- Prin intermediul monitorizării automate a vulnerabilităților, puteți verifica și remedia vulnerabilitățile detectate, în fereastra **Notificări**.

Ar trebui să verifici și să remediezi vulnerabilitățile sistemului săptămânal sau o dată la două săptămâni.

Scanarea sistemului pentru identificarea vulnerabilităților

Pentru a detecta vulnerabilitățile sistemului, Bitdefender necesită o conexiune activă la internet.

Pentru a-ți scana sistemul în vederea identificării vulnerabilităților:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **VULNERABILITATE**, apasă pe **Deschide**.
3. În secțiunea **Scanare vulnerabilitate** fă clic pe **Inițiere scanare**, apoi așteaptă ca Bitdefender să verifice dacă există vulnerabilități în sistem. Vulnerabilitățile detectate sunt grupate în trei categorii:

   - **SISTEM DE OPERARE**

     - **Securitatea sistemului de operare**
       Setările modificate ale sistemului care îți pot compromite dispozitivul și datele, cum ar fi avertismentele afișate când fișierele executate efectuează modificări asupra sistemului fără permisiunea ta sau când dispozitivele MTP, cum ar fi telefoanele sau camerele, se conectează și execută diferite operațiuni fără știrea ta.

     - **Actualizări Windows importante**
       Se afișează o listă de actualizări Windows importante care nu sunt instalate pe computerul tău. Ar putea fi necesară repornirea sistemului pentru a permite finalizarea instalării de către Bitdefender. Reține că instalarea actualizărilor poate dura câteva minute.

     - **Conturi Windows vulnerabile**
       Poți vedea lista conturilor de utilizator Windows configurate pe dispozitivul tău și nivelul de protecție asigurat de parola acestora. Puteți să-i solicitați utilizatorului să schimbe parola la următoarea autentificare sau puteți schimba dumneavoastră parola imediat. Pentru a seta o nouă parolă pentru sistemul tău, selectează **Schimbă parola acum**.

Pentru a crea o parolă puternică, îți recomandăm să utilizezi o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

- **APLICAȚII**
  - **Securitatea browserului**
    Modificări ale setărilor dispozitivului tău care permit executarea fișierelor și programelor descărcate prin Internet Explorer fără o validare a integrității, ceea ce ar putea conduce la compromiterea dispozitivului tău.
  - **Actualizări aplicații**
    Pentru a vedea informațiile despre aplicația care urmează a fi actualizată, clic pe numele acesteia din listă.
    Dacă o aplicație nu este la zi, accesează **Descărcare versiune nouă** pentru a descărca versiunea ce mai recentă.
- **REȚEA**
  - **Rețea și date de conectare**
    Setările modificate ale sistemului cum ar fi conectarea automată la rețele hotspot nesecurizate fără știrea ta sau neefectuarea criptării asupra traficului de ieșire prin canalul securizat.
  - **Rețele Wi-Fi și routere**
    Pentru a afla mai multe despre rețeaua wireless și routerul la care ești conectat, clic pe numele acesteia din listă. Dacă se recomandă să setezi o parolă mai puternică pentru rețeaua ta de acasă, asigură-te că urmezi instrucțiunile noastre, astfel încât să poți rămâne conectat fără să-ți faci griji cu privire la confidențialitatea datelor tale.
    Atunci când sunt disponibile și alte recomandări, urmează instrucțiunile pentru a te asigura că rețeaua ta de acasă este protejată de ochii iscoditori ai hackerilor.

Cu ajutorul monitorizării automate a vulnerabilităților

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

Pentru a verifica și soluționa problemele detectate:

1. Clic **Notificări** pe meniul de navigare de pe Interfața Bitdefender.
2. În fila **Toate**, selectează notificarea privind scanarea Vulnerabilităților.
3. Puteți vizualiza informații detaliate cu privire la vulnerabilitățile sistemului detectate. În funcție de problemă, pentru a remedia o anumită vulnerabilitate, procedați după cum urmează:
   - Dacă sunt disponibile actualizări Windows, efectuează clic pe **Instalare**.
   - Dacă actualizarea automată Windows este dezactivată, faceți clic **Activare**.
   - Dacă o aplicație nu este actualizată, efectuează clic pe **Actualizează acum** pentru a găsi un link către pagina furnizorului, de unde poți instala cea mai recentă versiune a aplicației respective.
   - Dacă un cont de utilizator Windows are o parolă slabă, faceți clic pe **Modificare 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 **Remediere** pentru a o dezactiva.
   - Dacă routerul pe care l-ai configurat are configurată o parolă slabă, efectuează clic pe **Modificare parolă** pentru a accesa interfața din care poți configura o parolă puternică.
   - Dacă rețeaua la care ești conectat conține vulnerabilități care pot supune sistemul tău unor riscuri, fă clic pe **Modificare setări Wi-Fi**.

Pentru a configura setările de monitorizare a vulnerabilităților:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **VULNERABILITATE** panou, faceți clic **Deschis**.

> **Important**
> Pentru a primi informări automate cu privire la vulnearibilitățile sistemului sau aplicației, mențineți opțiunea **Vulnerabilitate** activată.

3. Mergi la fila **Setări**.
4. Selectează vulnerabilitățile sistemului care dorești să fie verificate în mod regulat, cu ajutorul comutatoarelor corespunzătoare.

   Actualizări Windows

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

   Actualizări ale aplicației

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

   Parolele utilizatorului

   Verifică dacă parolele pentru conturile de Windows și routerele 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 @).

   Autoplay

   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 amenințări 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.

   Funcția Asistență Securitate Wi-Fi

   Verifică dacă rețeaua wireless de acasă la care ești conectat este sigură sau nu și dacă are vulnerabilități. De asemenea, verifică dacă parola routerului de acasă este suficient de puternică și află cum o poți face mai sigură.

   Majoritatea rețelelor wireless neprotejate sunt nesigure, permițând astfel hackerilor să aibă acces la activitățile tale private.

Notă
Dacă dezactivezi monitorizarea pentru o anumită vulnerabilitate, posibilele probleme aferente nu vor mai fi înregistrate în fereastra Notificări.

Evaluare securitate Wi-Fi

Atunci când te deplasezi, lucrezi dintr-o cafenea sau aștepți în aeroport, conectarea la o rețea wireless publică pentru a face plăți, verifica e-mail-ul sau conturile pe rețelele sociale poate fi soluția cea mai rapidă. Însă pot exista curioși care să încerce să-ți fure datele personale, urmărind informațiile care trec prin rețea.

Datele personale includ parolele și numele de utilizator pe care le folosești pentru a-ți accesa conturile online, cum ar fi căsuțele de e-mail, conturile bancare, conturile de rețele sociale, dar și mesajele pe care le trimiți.

De obicei, rețelele wireless publice sunt cel mai probabil nesigure deoarece nu necesită parolă la autentificare sau, dacă au parolă, aceasta poate fi pusă la dispoziția oricui dorește să se conecteze. Mai mult, pot exista rețele periculoase sau de tip honeypot, care reprezintă o țintă pentru infractorii cibernetici.

Asistentul de securitate Bitdefender pentru Wi-Fi îți oferă informații despre:

- **Rețelele Wi-Fi de acasă**
- **Rețelele Wi-Fi de birou**
- **Rețelele Wi-Fi publice**

Activarea sau dezactivarea notificărilor pentru Asistență Securitate Wi-Fi

Pentru a activa sau dezactiva notificările pentru Asistență Securitate Wi-Fi:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **VULNERABILITATE** panou, faceți clic **Deschis**.
3. Mergi la fereastra **Setări** și activează sau dezactivează opțiunea **Asistent de securitate Wi-Fi**.

Configurarea rețelei Wi-Fi de acasă

Pentru a porni configurarea rețelei tale de acasă:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **VULNERABILITATE** panou, faceți clic **Deschis**.
3. Accesează fereastra **Asistent de securitate Wi-Fi** și selectează **Wi-Fi acasă**.
4. În fila **Wi-Fi acasă** apasă pe **SELECTEAZĂ WI-FI ACASĂ**.
   Se va afișa o listă a rețelelor wireless la care te-ai conectat până în prezent.
5. Găsește rețeaua ta de acasă și apoi fă clic pe **SELECTEAZĂ**.

Dacă o rețea de acasă este considerată nesecurizată sau nesigură, sunt afișate recomandări de configurare pentru îmbunătățirea securității.

Pentru a șterge rețeaua wireless pe care ai setat-o ca fiind rețeaua ta de acasă, fă clic pe butonul **ȘTERGERE**.

Pentru a adăuga o nouă rețea wireless ca rețea de acasă, accesează opțiunea **Selectează o nouă rețea Wi-Fi acasă**.

Configurarea rețelei Wi-Fi de acasă

Pentru a începe configurarea rețelei tale de la birou:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În **VULNERABILITATE** panou, faceți clic **Deschis**.
3. Accesează fereastra **Asistent de securitate Wi-Fi** și selectează **Wi-Fi birou**.
4. În fila **Wi-Fi birou** apasă pe **SELECTEAZĂ WI-FI BIROU**.
   Se afișează o listă cu rețelele wireless la care v-ați conectat până acum.
5. Găsește rețeaua ta de la birou și apoi clic pe **SELECTEAZĂ**.

Dacă o rețea de birou este considerată nesecurizată sau nesigură, sunt afișate recomandări de configurare pentru îmbunătățirea securității.

Pentru a șterge rețeaua wireless pe care ai setat-o ca fiind rețeaua ta de birou, accesează opțiunea **ȘTERGE**.

Pentru a adăuga o nouă rețea wireless ca rețea de birou, accesează opțiunea **Selectează o nouă rețea Wi-Fi de birou**.

Wi-Fi Public

Atunci când ești conectat la o rețea nesecurizată sau nesigură, este activat profilul Wi-Fi public. Cât timp acest profil este activ, Bitdefender Ultimate Small Business Security este configurat pentru a pune în aplicare automat următoarele setări:

- Funcția Advanced Threat Defense este activă
- Firewall-ul Bitdefender este pornit și următoarele setări sunt aplicate adaptorului tău wireless:
  - Mod ascuns - PORNIT
  - Tipul rețelei - Public
- Următoarele setări din Online Threat Prevention sunt activate:
  - Scanare web criptată
  - Protecție împotriva fraudelor
  - Protecție împotriva tentativelor de phishing
- Este disponibil un buton care deschide Bitdefender Safepay™. În acest caz, protecția Hotspot pentru rețele nesecurizate este activată în mod implicit.

Verifică informațiilor despre rețelele Wi-Fi

Pentru a verifica informațiile despre rețelele wireless la care te conectezi de obicei:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **VULNERABILITATE** panou, faceți clic **Deschis**.
3. Accesează fereastra **Asistent de securitate Wi-Fi**.
4. În funcție de informațiile de care ai nevoie, selectează una dintre următoarele trei file: **Wi-Fi acasă**, **Wi-Fi birou** sau **Wi-Fi publică**.
5. Fă clic pe **Vizualizare detalii** din dreptul rețelei despre care dorești să afli mai multe informații.

Există trei tipuri de rețele wireless filtrate în funcție de importanța lor, fiecare marcat printr-o anumită pictogramă:

Wi-Fi nu este sigur - indică faptul că nivelul de securitate al rețelei este prea scăzut. Acest lucru înseamnă că utilizarea rețelei prezintă un

risc ridicat și nu este recomandată pentru efectuarea de plăți sau pentru verificarea conturilor bancare fără o protecție suplimentară. În astfel de situații, îți recomandăm să utilizezi Bitdefender Safepay™ cu protecție Hotspot pentru rețelele nesigure activate.

Wi-Fi nu este sigur - indică faptul că nivelul de securitate al rețelei este moderat. Acest lucru înseamnă că poate prezenta vulnerabilități și nu este recomandată pentru efectuarea de plăți sau pentru verificarea conturilor bancare fără o protecție suplimentară. În astfel de situații, îți recomandăm să utilizezi Bitdefender Safepay™ cu protecție Hotspot pentru rețelele nesigure activate.

Wi-Fi este sigur - indică faptul că rețeaua pe care o utilizezi este sigură. În acest caz, poți folosi date sensibile pentru a realiza operațiuni online.

Atunci când efectuați clic pe link-ul **Vizualizare detalii** din dreptul fiecărei rețele, se afișează următoarele detalii:

- **Securizate** - aici puteți vedea dacă rețeaua selectată este securizată sau nu. Rețelele necriptate pot face ca datele pe care le folosești să fie expuse.
- **Tip de criptare** - aici poți vedea tipul de criptare folosit de rețeaua selectată. Unele tipuri de criptare pot fi nesigure. Prin urmare, îți recomandăm să verifici informațiile despre tipul de criptare afișat pentru a te asigura că ești protejat în timp de navighezi pe internet.
- **Canal/Frecvență** - aici poți vizualiza frecvența canalului utilizat de rețeaua selectată.
- **Complexitatea parolei** - aici poți vedea cât de puternică este parola. Te rugăm să reții că rețelele cu parole slabe reprezintă o țintă pentru infractorii cibernetici.
- **Tipul autentificării** - aici poți verifica dacă rețeaua selectată este sau nu protejată prin parolă. Se recomandă să te conectezi numai la rețele cu parole puternice.
- **Tip de autentificare** - aici poți vedea tipul de autentificare folosit de rețeaua selectată.

3.2.8. Protecție video și audio

Tot mai multe amenințări sunt construite să acceseze camerele web și microfoanele integrate. Pentru a împiedica accesul neautorizat la camera

ta web și pentru a te informa ce aplicații nesigure accesează microfonul dispozitivului tău și când, Bitdefender Video&Audio include:

- **Protecție pentru camera web**
- **Monitorizarea microfonului**

Protecție cameră web

Faptul că hackerii pot prelua controlul asupra camerei tale web pentru a te spiona nu mai este o noutate, însă soluțiile menite să te apere, precum revocarea drepturilor de acces ale aplicațiilor, dezactivarea camerei dispozitivului sau acoperirea acesteia, nu sunt foarte practice. Pentru a împiedica tentativele de acces la viața ta privată, Bitdefender Webcam Protection monitorizează constant aplicațiile care încearcă să obțină accesul la camera ta și le blochează pe cele care nu sunt considerate a fi de încredere.

Ca măsură de siguranță, vei fi notificat de fiecare dată când o aplicație nesigură va încerca să obțină acces la camera ta.

Activarea sau dezactivarea funcției Webcam Protection

1. Apasă pe **Confidențialitate** din meniul de navigare al **interfeței Bitdefender**.
2. În fila **PROTECȚIE VIDEO ȘI AUDIO**, fă clic pe **Setări**.
3. Acum mergi la fereastra **Setări** și activează sau dezactivează butonul corespunzător.

Configurarea funcției Webcam Protection

Acum poți configura ce reguli să fie aplicate atunci când o aplicație încearcă să obțină acces la camera ta web, urmând acești pași:

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
2. În **PROTECTIE VIDEO & AUDIO** panou, faceți clic **Setări**.
3. Du-te la **Setări** fila.

Sunt disponibile următoarele opțiuni:

Reguli de blocare a aplicațiilor

- **Blochează orice acces la camera web** - nicio aplicație nu va putea accesa camera dvs. web.
- **Blocarea accesului browserelor la camera web** - nu se permite niciunui alt browser web, cu excepția Internet Explorer și Microsoft Edge, să aibă acces la camera ta web. Din cauza procedurii de executare a aplicațiilor Windows Store într-un singur proces, Internet Explorer și Microsoft Edge nu pot fi detectate de Bitdefender ca browsere web și, prin urmare, sunt exceptate de la această setare.
- **Setează drepturile de acces pentru aplicații pe baza preferințelor comunității** - dacă majoritatea utilizatorilor Bitdefender consideră o aplicație utilizată în mod frecvent ca fiind inofensivă, atunci accesul acesteia la camera web va fi setat automat pe Permite. Dacă o aplicație folosită în mod frecvent este considerată ca fiind periculoasă de mulți utilizatori, atunci accesul acesteia va fi setat automat pe Blocat.

Notificări

- **Notificare în momentul în care aplicațiile permise se conectează la camera web** - vei fi notificat de fiecare dată când o aplicație permisă îți va accesa camera web.

Adăugarea aplicațiilor în lista Webcam Protection

Aplicațiile care încearcă să se conecteze la camera web sunt detectate automat în funcție de comportamentul lor și preferințele comunității, iar accesul acestora este permis sau blocat. Cu toate acestea, puteți configura manual ce acțiune doriți să fie întreprinsă urmând acești pași:

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
2. În panoul **PROTECTIE VIDEO & AUDIO**, faceți clic pe **Setări**.
3. Selectează fereastra **Protecția cameră web**.
4. Selectează fereastra **Adaugă aplicație**.
5. Efectuează clic pe link-ul dorit:
   - **Din Windows Store** - se afișează o listă cu aplicațiile detectate din Windows Store. Activează butoanele de lângă aplicațiile pe care dorești să le adaugi pe listă.

- **Din aplicațiile tale** - mergi la fișierul .exe pe care vrei să-l adaugi și apoi apasă pe **OK**.

Pentru a vedea opțiunea utilizatorilor Bitdefender pentru aplicația selectată, fă clic pe pictograma .

În această fereastră se vor afișa aplicațiile care vor solicita acces la camera web, alături de data și ora ultimei activități.

Vei fi notificat de fiecare dată când una dontre aplicațiile permise este blocată de către utilizatrii Bitdefender.

Pentru a bloca accesul unei aplicații adăugate pe listă la camera ta web, fă clic pe pictograma .

Pictograma se transformă în , ceea ce înseamnă că aplicația selectată nu va avea acces la camera dvs. web.

Monitorizare microfon

Aplicațiile de tip rogue pot accesa microfonul inclus în mod silențios sau în fundal fără consimțământul dvs. Pentru a te face conștient cu privire la posibilele programe malițioase de tip exploits, monitorizare Microfon te va notifica despre aceste evenimente. Astfel, nicio aplicație nu va putea obține acces la microfonul dvs. fără ca dvs. să știți acest lucru.

Activarea sau dezactivarea monitorului pentru Microfon

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
2. În **PROTECTIE VIDEO & AUDIO** panou, faceți clic **Setări**.
3. Selectează **Setări** fereastră.
4. În fereastra **Setări**, activează sau dezactivează butonul **Monitorizare microfon**.

Configurarea notificărilor pentru monitorul de Microfon

Pentru a configura ce notificări ar trebui să apară când aplicațiile încearcă să obțină acces la microfonul dvs., urmați pașii de mai jos:

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.

2. În **PROTECTIE VIDEO & AUDIO** panou, faceți clic **Setări**.
3. Du-te la **Setări** fereastră.

Notificări

- **Anunță-mă atunci când aplicația încearcă să acceseze microfonul**
- **Anunță-mă atunci când browser-ele accesează microfonul**
- **Anunță-mă atunci când aplicații nesecurizate îmi accesează microfonul**
- **Afișați notificația în baza alegerii utilizatorilor Bitdefender**

Adăugarea de aplicații în lista de monitorizare a Microfonului

Aplicațiile care vor încerca să se conecteze la microfonul dvs. vor fi detectate automat și adăugate la lista de Notificări. Cu toate acestea, puteți configura manual individual dacă o notificare trebuie afișată sau nu prin respectarea următorilor pași:

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
2. În **PROTECTIE VIDEO & AUDIO** panou, faceți clic **Setări**.
3. Mergi la fereastra **Protecție audio**.
4. Clic **Adăugați aplicația** fereastră.
5. Faceți clic pe linkul dorit:
   - **Din Magazinul Windows** - este afișată o listă cu aplicațiile Windows Store detectate. Activați comutatoarele de lângă aplicațiile pe care doriți să le adăugați la listă.
   - **Din aplicațiile dvs** - accesați fișierul .exe pe care doriți să îl adăugați la listă, apoi faceți clic **Bine**.

Pentru a vedea ce au ales utilizatorii Bitdefender să facă cu aplicația selectată, faceți clic pe pictograma.

În această fereastră se vor afișa aplicațiile care vor solicita acces la microfon, alături de data și ora ultimei activități.

Pentru a nu mai primi notificări legate de activitatea unei aplicații adăugate pe listă, apasă pe pictograma.

Pictograma se transformă în , ceea ce înseamnă că nicio notificare Bitdefender nu va fi afișată când aplicația selectată va încerca să vă acceseze microfonul.

3.2.9. Remediere ransomware

Bitdefender Ransomware Remediation creează backupuri pentru fișierele tale precum documente, fotografii, videoclipuri sau muzică pentru a se asigura că sunt protejate împotriva distrugerii sau pierderii lor în cazul unui atac prin criptare ransomware. De fiecare dată când se detectează un atac ransomware, Bitdefender va bloca toate procesele implicate în atac și va începe procesul de remediere. În acest fel, vei putea să recuperezi conținutul tuturor fișierelor tale fără să plătești suma solicitată de răscumpărare.

Activarea sau dezactivarea funcției Remediere ransomware

Pentru a activa sau dezactiva funcția Remediere ransomware:

1. 1. Apasă pe **Protecție** în meniul de navigare al **interfeței Bitdefender**.
2. În secțiunea **REMEDIERE RANSOMWARE**, activează sau dezactivează opțiunea.

> **Notă**
> Pentru a te asigura că fișierele tale sunt protejate împotriva atacurilor ransomware, îți recomandăm să păstrezi activă opțiunea Remediere ransomware.

Activarea sau dezactivarea restabilirii automate

Restabilirea automată se asigură că fișierele tale sunt restabilite automat în eventualitatea unei criptări ransomware.

Pentru a activa sau dezactiva restabilirea automată:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **REMEDIERE RANSOMWARE**, fă clic pe **Administrare**.
3. În fereastra Setări, activează sau dezactivează butonul **Restabilire automată**.

Vizualizarea fișierelor restabilite automat

Atunci când opțiunea **Restabilire automată** este activată, Bitdefender va restabili automat fișierele criptate de ransomware. Astfel, te poți bucura

de o experiență fără griji de utilizare a dispozitivului știind că fișierele tale sunt în siguranță.

Pentru a vizualiza fișierele care au fost restabilite automat:

1. Clic **Notificări** din meniul de navigare de pe Interfața Bitdefender.
2. În fila **Toate**, selectează notificarea privind cel mai recent comportament ransomware remediat, apoi apasă pe **Fișiere restabilite**.
   Este afișată lista fișierelor restabilite. Tot aici poți vedea și locația în care au fost restabilite fișierele tale.

Restabilirea manuală a fișierelor criptate

În cazul în care trebuie să restabilești manual fișierele criptate de ransomware, urmează acești pași:

1. Clic **Notificări** pe meniul de navigare de pe Interfața Bitdefender.
2. În fila **Toate**, selectează notificarea privind cel mai recent comportament ransomware detectat, apoi apasă pe **Fișiere criptate**.
3. Este afișată lista fișierelor criptate.
   Selectează **Recuperare fișiere** pentru a continua.
4. În cazul în care procesul de restabilire eșuează, fie complet, fie parțial, trebuie să selectezi locația în care să fie salvate fișierele decriptate. Selectează **Restabilire locație** și apoi alege o locație din PC-ul tău.
5. Va apărea o fereastră de confirmare.
   Selectează **Finalizare** pentru a finaliza procesul de restabilire.

Fișierele cu următoarele extensii pot fi restabilite în cazul în care sunt criptate:

.3g2;.3gp;.7z;.ai;.aif;.arj;.asp;.aspx;.avi;.bat;.bin;.bmp;.c;.cda;.cgi;.class;.com;.cpp;.cs;.css;.csv;.dat;.db;.dbf;.deb;.doc;.docx;.gif;.gz;.h264;.h;.flv;.htm;.html;.ico;.jar;.java;.jpeg;.jpg;.js;.jsp;.key;.m4v;.mdb;.mid;.midi;.mkv;.mp3;.mp4;.mov;.mpg;.mpeg;.ods;.odp;.odt;.ogg;.pdf;.pkg;.php;.pl;.png;.pps;.ppt;.pptx;.ps;.psd;.py;.rar;.rm;.rtf;.sav;.sql;.sh;.svg;.swift;.swf;.tar;.tex;.tif;.tiff;.txt;.xlr;.xls;.xlsx;.xml;.wmv;.vb;.vob;.wav;.wks;.wma;.wpl;.wps;.wpd;.wsf;.z;.zip;

Adăugarea aplicațiilor în lista de excepții

Poți configura reguli de excepțare pentru aplicațiile sigure astfel încât funcția Remediere ransomware să nu le blocheze dacă efectuează acțiuni specifice programelor ransomware.

Pentru a adăuga aplicații în lista de excepții a funcției Remediere ransomware:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **REMEDIERE RANSOMWARE** panou, faceți clic **Administra**.
3. Accesează fereastra **Excepții** și selectează **+Adaugă o excepție**.

3.2.10. Cryptomining Protection

Ce este Cryptomining Protection?

Prin utilizarea criptominării, atacatorii pot beneficia financiar fără a suporta costurile și consecințele legale aferente.

Caracteristica Bitdefender Cryptomining Protection apără computerele Windows împotriva amenințării tot mai mari ale activităților de criptomining neautorizate, o practică rău intenționată care exploatează resursele și electricitatea unui utilizator pentru a genera venituri pentru atacatori.

Notă

Protecția împotriva criptominării se bazează pe:

- Bitdefender Shield
- Prevenirea atacurilor web

Pentru a putea rula Cryptomining Protection, ambele două funcții trebuie să fie și ele activate.

Activarea protecției criptominării

Caracteristica Criptomining Protection se află în fila Protecție.

Pentru a-l activa, comutați pur și simplu comutatorul corespunzător.

Notă

Protecția Cryptomining este dezactivată în mod implicit, asigurând că utilizatorii au control asupra activării acesteia.

Moduri de operare

Odată activată, caracteristica Cryptomining Protection operează în 2 stări distincte, fiecare adaptată preferințelor utilizatorului:

1. **Blocați toate activitățile de Cryptomining.** (blochează automat orice activitate de cripto-mining și ia măsurile necesare pentru a preveni alte încercări neautorizate)
   Acest mod este ideal pentru utilizatorii care nu au intenția de a se angaja în activități de cripto-mining.
2. **Detectați activitățile de criptomining.** (emite alerte ori de câte ori este detectată o activitate de cripto-mining și necesită intrarea utilizatorului pentru a determina acțiunea corespunzătoare)
   Acest mod este potrivit pentru utilizatorii implicați activ în propriile activități de cripto-mining, dar care doresc să monitorizeze și să controleze orice încercări neautorizate.

Gestionați excepțiile

Pot fi specificate excepții pentru aplicații, cu capacitatea adăugată de a defini linii de comandă specifice. Totuși, pot fi stabilite și excepții fără a fi nevoie de furnizarea unor astfel de parametri detaliați, oferind un echilibru între personalizare și simplitate.

Pentru a adăuga o excepție:

1. Clic**Protecție**în meniul din partea stângă a interfeței Bitdefender.
2. În**Protecție împotriva criptominării**panou, faceți clic**Setări**.
3. Apasă pe**Gestionați excepțiile**opțiune.
4. Apoi, faceți clic pe**Adăugați o excepție**buton.
5. Se va deschide o nouă fereastră. Puteți exclude manual aplicații, adrese URL și adrese IP.
6. În cele din urmă, faceți clic**Salvați**. Noua regulă este adăugată la lista de excepții Cryptomining Protection.

> **Notă**
> Pentru a elimina o excepție, faceți clic pe pictograma coș de gunoi de lângă ea.

3.2.11. Anti-tracker

Multe dintre site-urile web pe care le accesezi utilizează instrumente de urmărire de tip tracker pentru a colecta informații despre comportamentul tău, fie pentru a le distribui unor companii terțe, fie pentru a afișa anunțuri mai relevante pentru tine. Astfel, proprietarii site-urilor web fac bani pentru a putea oferi conținut gratuit sau pentru a continua să funcționeze. Pe lângă colectarea de informații, tracker-ele pot încetini experiența ta de navigare sau îți pot afecta lățimea de bandă.

Când extensia Bitdefender Anti-tracker este activată în browserul web, aceasta te ajută eviți să fii monitorizat, astfel încât datele tale rămân confidențiale în timp ce navighezi online, precum și să reduci timpul necesar pentru încărcarea site-urilor web.

Extensia Bitdefender este compatibilă cu următoarele browsere web:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

Tracker-ele pe care le detectăm sunt grupate în următoarele categorii:

- **Publicitate** - se utilizează pentru a analiza traficul de pe site-urile web, comportamentul utilizatorilor sau tiparele de trafic generat de utilizatori.
- **Interacțiunea cu clienții** - se utilizează pentru a măsura interacțiunea utilizatorilor cu diferite forme de introducere de informații, cum ar fi chat sau suport.
- **Esențiale** - se utilizează pentru a monitoriza funcționalitățile de importanță critică ale paginilor web.
- **Date de analiză site** - se utilizează pentru a colecta date referitoare la utilizarea paginilor web.
- **Rețele de socializare** - se utilizează pentru a monitoriza audiența pe rețelele de socializare, activitatea și implicarea utilizatorilor pentru diferite platforme de socializare.

Interfața Anti-tracker

Când extensia Bitdefender Anti-tracker este activată, pictograma apare lângă bara de căutare din browserul tău web. De fiecare dată când vizitezi

un site web, pe pictogramă vei observa un număr care se referă la trackerele detectate și blocate. Pentru a vizualiza mai multe detalii despre trackerele blocate, apasă pe pictogramă pentru a deschide interfața. În afară de numărul de trackere blocate, poți vizualiza și timpul necesar pentru încărcarea paginii și categoriile din care fac parte trackerele detectate. Pentru a vizualiza lista de site-uri web care sunt urmărite, apasă pe categoria respectivă.

Pentru a dezactiva funcția Bitdefender de blocare a tracker-elor pe site-ul pe care îl accesați în momentul respectiv, selectează opțiunea **Întrerupeți protecția pe acest site**. Această setare se aplică numai atâta timp cât site-ul este deschis și va reveni automat la starea inițială după ce părăsești site-ul web.

Pentru a permite tracker-elor dintr-o anumită categorie să îți monitorizeze activitatea, selectează activitatea dorită și apoi clic pe butonul corespunzător. Dacă te răzgândești, apasă din nou pe același buton.

Dezactivarea Bitdefender Anti-tracker

Pentru a dezactiva modulul Bitdefender Anti-tracker:

- Din browserul dvs. web:
  1. Deschideți browser-ul web.
  2. Apasă pe pictograma de lângă bara de adresă din browserul web.
  3. Apasă pe pictograma din colțul din dreapta sus.
  4. Utilizează butonul corespunzător pentru dezactivare.
     Pictograma Bitdefender devine gri.

- Din interfața Bitdefender:
  1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
  2. În secțiunea **ANTI-TRACKER**, fă clic pe **Setări**.
  3. Dezactivează butonul corespunzător din dreptul browserului web pentru care dorești să dezactivezi extensia.

Permiterea urmăririi unui site web

Dacă dorești ca activitatea ta să fie urmărită în timp ce accesezi un anumit site web, poți adăuga adresa acestuia în lista de excepții, după cum urmează:

1. Deschideți browserul web.
2. Apasă pe pictograma de lângă bara de căutare.
3. Apasă pe pictograma din colțul din dreapta sus.
4. Dacă te afli pe site-ul web pe care dorești să-l adaugi la excepții, selectează opțiunea **Adaugă în listă acest site web**.
   Dacă dorești să adaugi un alt site web, introdu adresa acestuia în câmpul corespunzător și apoi selectează .

3.2.12. Securitate Safepay pentru tranzacțiile online

Calculatorul a început să devină principalul instrument 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™ este, în primul rând, un browser protejat, un mediu izolat proiectat să se asigure că operațiunile bancare, cumpărăturile și orice alte tipuri de tranzacții online pe care le efectuezi sunt confidențiale și securizate.

Bitdefender Safepay™ vă oferă următoarele funcții:

- Blochează accesul la calculatorul tău și orice încercări de a realiza capturi ale ecranului tău.
- Include o tastatură virtuală care, dacă este utilizată, nu permite hackerilor să citească ceea ce introduci de pe aceasta.
- Este complet idependentă de celelalte browsere ale tale.

- Include protecție pentru punctele wireless de acces la Internet încorporată pe care o poți utiliza în cazul conectării la rețele Wi-fi nesecurizate.
- Acceptă marcajele și îți permite să navighezi pe site-urile tale preferate de tranzacții bancare/cumpărături.
- Nu se limitează la tranzacții bancare și cumpărături online. Cu Bitdefender Safepay™, poți deschide orice site web.

Cum să utilizezi Bitdefender Safepay™

În mod implicit, Bitdefender detectează dacă navighezi către un site de tranzacții online sau de cumpărături online în orice browser de pe dispozitivul tău și îți solicită să îl lansezi în Bitdefender Safepay™.

Pentru a accesa interfața principală a Bitdefender Safepay™, folosește una dintre următoarele metode:

- Din **interfața Bitdefender**:
  1. Clic **Confidențialitate** din meniul de navigare de pe Interfața Bitdefender.
  2. În secțiunea **SAFEPAY**, fă clic pe **Setări**.
  3. În fereastra **Safepay**, fă clic pe **Lansează Safepay**.
- Din Windows:
  - În **Windows 7**:
    1. Apasă pe **Pornire** și accesează **Toate programele**.
    2. Fă clic pe **Bitdefender**.
    3. Fă clic pe **Bitdefender Safepay™**.
  - În **Windows 8** și **Windows 8.1**:
    Localizați Bitdefender Safepay™ din ecranul de Start Windows (de exemplu, puteți tasta "Bitdefender Safepay™" direct pe ecranul de Start) și apoi faceți clic pe pictograma.
  - În **Windows 10** și **Windows 11**:
    Introduceți "Bitdefender Safepay™" în caseta de căutare din bara de sarcini și faceți clic pe pictogramă.

Dacă ești obișnuit cu browserele web, nu vei avea probleme în utilizarea Bitdefender Safepay ™- acesta arată și se comportă ca un browser obișnuit:

- introdu URL-urile pe care dorești să le accesezi în bara de adrese.
- adaugă file pentru a vizita mai multe site-uri web în fereastra Bitdefender Safepay™ apăsând pe ⊞.
- navighează și reîmprospătează paginile utilizând ← →, și respectiv ↻.
- accesează **setările** Bitdefender Safepay™ printr-un clic și selectează **Setări**.
- administrează-ți **marcajele** făcând clic pe ☆ de lângă bara pentru adrese.
- deschide tastatura virtuală apăsând pe ⌨.
- mărește sau micșorează dimensiunea browserului apăsând simultan tastele **Ctrl** și **+/-** de pe tastatura numerică.
- vizualizează informații despre produsul tău Bitdefender făcând clic pe ⋯ și selectând **Despre**.
- printează informații importante făcând clic pe ⋯ și selectând **Tipărire**.

> **Notă**
> Pentru a comuta între Bitdefender Safepay™ și desktopul Windows, apasă tastele **Alt+Tab** sau fă clic pe opțiunea **Comută pe Desktop** din colțul din stânga sus al ferestrei.

Configurarea setărilor

Fă clic pe ⋯ și selectează **Setări** pentru a configura Bitdefender Safepay™:

Aplică regulile Bitdefender Safepay pentru domeniile accesate

Aici vor apărea site-urile web pe care le-ai adăugat la **Bookmarks** cu opțiunea **Deschidere automată în Safepay** activată. Dacă dorești să dezactivezi deschiderea automat cu Bitdefender Safepay™ a unui site web din listă, clic pe × din dreptul înregistrării dorite din coloana **Ștergere**.

Blochează ferestre pop-up

Poți opta pentru blocarea pop-up-urilor făcând clic pe comutatorul corespunzător.

De asemenea, puteți crea o listă a site-urilor pe care permiteți afișarea pop-up-urilor. Este recomandat ca lista să conțină doar site-uri web în care aveți deplină încredere.

Pentru a adăuga un site în listă, introdu adresa acestuia în câmpul corespunzător și efectuează clic pe **Adaugă domeniu**.

Pentru a șterge un site web din listă, selectează x-ul corespunzător înregistrării dorite.

Administrare plugin-uri

Poți opta pentru activarea sau dezactivarea anumitor plugin-uri din Bitdefender Safepay™.

Administrare certificate

Poți importa certificate din sistemul tău într-un magazin de certificate.

Selectează **IMPORT** și urmează instrucțiunile asistentului pentru a utiliza certificatele în Bitdefender Safepay™.

Utilizează tastatura virtuală

Tastatura virtuală va apărea automat atunci când este selectat un câmp de parolă.

Folosește butonul corespunzător pentru a activa sau dezactiva această funcție.

Confirmarea tipăririi

Activează această opțiune dacă dorești să confirmi înainte ca procesul de tipărire să înceapă.

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. Fă clic pe ⋯ și selectează **Marcaje** 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 apoi faceți clic pe **CREEAZĂ**. Faceți clic pe opțiunea **Deschide automat în Safepay** dacă doriți ca pagina marcată să se deschidă cu Bitdefender Safepay™ de fiecare dată când o accesați. URL-ul este și el adăugat la lista Domeniilor de pe pagina setări.

Dezactivarea notificărilor Safepay

Când este detectat un site bancar, produsul Bitdefender este setat să te notifice prin intermediul unei ferestre pop-up.

Pentru a dezactiva notificările Safepay:

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
2. În **SAFEPAY** panou, faceți clic **Setări**.
3. În fereastra **Setări**, dezactivează butonul din dreptul **Notificări Safepay**.

3.2.13. Antifurt dispozitiv

Furtul de laptop este o problemă majoră care afectează atât persoanele, cât și organizațiile. Chiar mai mult decât pierderea hardware-ului în sine, datele pierdute cu acesta pot provoca daune semnificative, atât financiar, cât și emoțional.

Cu toate acestea, puțini oameni iau măsurile adecvate pentru a-și asigura datele personale, de afaceri și financiare importante în caz de furt sau pierdere.

Bitdefender Anti-Theft vă ajută să fiți mai bine pregătiți pentru un astfel de eveniment, permițându-vă să vă localizați sau să blocați laptopul de la distanță și chiar să ștergeți toate datele de pe acesta, în cazul în care vă despărțiți de laptop împotriva voinței dvs.

Pentru a utiliza funcțiile Antifurt, trebuie îndeplinite următoarele cerințe preliminare:

- Comenzile pot fi trimise numai din contul Bitdefender.
- Laptopul trebuie să fie conectat la internet pentru a primi comenzile.

Funcțiile antifurt funcționează în felul următor:

Localiza

Vizualizați locația dispozitivului dvs. pe Google Maps.

Precizia locației depinde de modul în care Bitdefender o poate determina. Locația este determinată la zeci de metri dacă Wi-Fi este activat pe laptop și există rețele wireless în raza de acțiune.

Dacă laptopul este conectat la o rețea LAN cu fir fără o locație bazată pe Wi-Fi disponibilă, locația va fi determinată pe baza adresei IP, care este considerabil mai puțin precisă.

Alerta

Trimiteți o alertă de la distanță pe dispozitiv.

Funcția este disponibilă numai pe dispozitivele mobile.

Lacăt

Blocați laptopul și setați un PIN de 4 cifre pentru deblocare. Când trimiteți **Lacăt** comanda, sistemul repornește și reconectarea în Windows este posibilă numai după introducerea codului PIN pe care l-ați setat.

Dacă doriți ca Bitdefender să facă fotografii cu cel care încearcă să aibă acces la laptopul dvs., bifați caseta de selectare corespunzătoare. Fotografiile realizate sunt realizate folosind camera frontală și afișate împreună cu marcajul de timp în tabloul de bord Anti-Theft. Vor fi salvate doar cele mai recente două fotografii.

Această acțiune este disponibilă numai pentru laptopurile care au cameră frontală.

Sterge

Eliminați toate datele din sistemul dvs. Când trimiteți **Sterge** comanda, laptopul repornește și datele de pe toate partițiile hard diskului sunt șterse.

Arată IP

Afișează ultima adresă IP pentru dispozitivul selectat. Clic **AFIȚI IP** pentru a-l face vizibil.

Antifurtul este activat după instalare și poate fi accesat exclusiv prin contul tău Bitdefender de pe orice dispozitiv conectat la internet, oriunde.

Utilizarea funcțiilor antifurt

Pentru a accesa funcțiile Anti-Theft, utilizați una dintre următoarele posibilități:

- Din interfața principală Bitdefender:
  1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
  2. Clic **MERGI LA CENTRAL**.
     Sunteți redirecționat către pagina Bitdefender Central. Asigurați-vă că sunteți conectat cu datele de conectare.
  3. În fereastra Bitdefender Central care se deschide, faceți clic pe cardul dispozitivului dorit, apoi selectați **Anti furt**.
- Pe orice dispozitiv cu acces la internet:
  1. Deschideți un browser web și accesați: https://central.bitdefender.com.
  2. Conectați-vă la contul dvs. Bitdefender folosind adresa de e-mail și parola.
  3. Selectează **Dispozitivele mele** panou.
  4. Faceți clic pe cardul dispozitivului dorit, apoi selectați **Anti furt**.
  5. Selectați funcția pe care doriți să o utilizați:
     Localiza - afișați locația dispozitivului dvs. pe Google Maps.
     Arată IP - afișați ultima adresă IP a dispozitivului dvs.
     Alerta - trimiteți o alertă pe dispozitiv.
     Lacăt - blocați laptopul și setați un cod PIN pentru deblocare.
     Sterge - ștergeți toate datele de pe laptop.

     Important
     După ce ștergeți un dispozitiv, toate funcțiile antifurt nu mai funcționează.

3.3. Utilități

3.3.1. Profiluri

Activitățile de serviciu zilnice, vizionarea filmelor sau jocurile pot încetini performanțele sistemului, cu precădere dacă rulează simultan cu procesele de actualizare Windows și sarcinile de actualizare. Cu Bitdefender, puteți acum alege și aplica profilul dorit, care efectuează ajustările sistemului adecvate pentru îmbunătățirea performanțelor aplicațiilor specifice instalate.

Bitdefender oferă următoarele profiluri:

- Profil de lucru
- Profil film
- Profilul jocului
- **Profil Wi-Fi publică**
- Profilul modului bateriei

Dacă decizi să nu utilizezi **Profiluri**, se activează un profil implicit numit **Standard**, care nu îți optimizează sistemul.

În funcție de activitatea ta, se aplică următoarele setări ale produsului la activarea unui profil Lucru, Film sau Joc:

- Toate alertele și pop-upurile BitDefender sunt dezactivate.
- Actualizarea automată este amânată.
- Scanările programate sunt amânate.
- Modulul antispam este activat.
- Modulul **Asistență pentru căutare** nu este disponibil.
- Notificările privind ofertele speciale sunt dezactivate.

În funcție de activitatea ta, se aplică următoarele setări ale sistemului la activarea unui profil Lucru, Film sau Joc:

- Actualizările automate Windows sunt amânate.
- Alertele și pop-up-urile Windows sunt dezactivate.
- Programele inutile care rulează în fundal sunt suspendate.
- Efectele vizuale sunt adaptate pentru performanțe superioare.

- Sarcinile de întreținere sunt amânate.
- Setările planului de alimentare sunt ajustate.

Cât timp Profilul Wi-Fi este activ, Bitdefender Ultimate Small Business Security este configurat pentru a pune în aplicare automat următoarele setări:

- Advanced Threat Defense este activată
- Paravanul de protecție Bitdefender este pornit și următoarele setări sunt aplicate adaptorului dvs. wireless:
  - Modul Stealth - PORNIT
  - Tip de rețea - Publică
- Următoarele setări din Prevenirea amenințărilor online sunt activate:
  - Scanare web criptată
  - Protecție împotriva fraudei
  - Protecție împotriva phishingului

Profil Lucru

Rularea mai multor sarcini la serviciu, cum ar fi trimiterea de e-mail-uri, comunicarea video cu colegi aflați la distanță sau lucrul cu aplicații de proiectare, vă pot afecta performanțele sistemului. Profilul de serviciu a fost proiectat pentru a vă ajuta să vă îmbunătățiți eficiența la lucru, prin dezactivarea unora dintre serviciile și sarcinile care rulează în fundal.

Configurarea profilului Serviciu.

Pentru a configura măsurile implementate în Profilul Lucru:

1. Clic **Utilități** din meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil Lucru.
4. Selectează ajustările sistemului care dorești să fie aplicate, prin bifarea opțiunilor de mai jos:
   - Crește performanța aplicațiilor de lucru
   - Optimizează setările de produs pentru Profilul Lucru

- Amână programele de fundal și activitățile de întreținere
- Amânare actualizare Windows automată

5. Efectuează clic pe **SALVEAZĂ** pentru a memora schimbările și a închide fereastra.

Adăugarea manuală a aplicațiilor la lista Profil Serviciu

Dacă Bitdefender nu intră automat în Profilul Serviciu când lansezi o anumită aplicație de serviciu, poți adăuga manual aplicația la **Lista aplicațiilor de lucru**.

Pentru a adăuga manual aplicații în Lista de aplicații de lucru din Profilul Serviciu:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Apasă pe **CONFIGURAȚI** butonul din zona Profil de lucru.
4. În fereastra **Setări profil lucru**, fă clic pe **Lista de aplicații**.
5. Fă clic pe **ADAUGĂ**.
   Se afișează o nouă fereastră. Mergeți la locația unde se găsește fișierul executabil, selectați-l și faceți clic pe **OK** pentru a-l adăuga în listă.

Profil Film

Afișarea videoclipurilor de calitate superioară, cum ar fi filmele de înaltă definiție, necesită resurse semnificative de sistem. Profilul Film adaptează setările sistemului și ale produsului, astfel încât să vă puteți bucura de o experiență plăcută și fără întreruperi.

Configurarea Profilului Film

Pentru a configura măsurile implementate în Profilul Film:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil film.
4. Alegeți ajustările sistemului pe care doriți să le aplicați, bifând următoarele opțiuni:

- Crește performanța aplicațiilor media
- Optimizează setările de produs pentru Profilul Film
- Amânați programele de fundal și sarcinile de întreținere
- Amânați actualizările automate Windows
- Ajustează configurările planului de energie pentru filme

5. Clic **SALVA** pentru a salva modificările și a închide fereastra.

Adăugarea manuală a dispozitivelor de redare video în lista Profil Film

Dacă Bitdefender nu intră automat în Profilul Film când lansați o anumită aplicație pentru redarea video clipurilor, puteți adăuga manual aplicația în **Lista aplicațiilor de film**.

Pentru a adăuga manual jucători video în lista Aplicațiilor de film din Profilul Film:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Apasă pe **CONFIGURAȚI** butonul din zona Profil film.
4. În fereastra **Setări profil film**, fă clic pe **Lista de playere**.
5. Clic **ADĂUGA**.
   Apare o nouă fereastră. Navigați la fișierul executabil al aplicației, selectați-l și faceți clic **Bine** pentru a-l adăuga pe listă.

Profil Joc

Pentru o experiență plăcută a jocului trebuie reduse încărcările de sistem și încetinirile. Folosind metoda euristică comportamentală, alături de o listă de jocuri cunoscute, Bitdefender poate detecta automat jocurile active și poate optimiza resursele sistemului pentru ca dvs. să vă puteți bucura de pauza de joc.

Configurarea Profilului Joc

Pentru a configura măsurile implementate în Profilul Joc:

1. Clic **Utilități** din meniul de navigare de pe Interfața Bitdefender.

2. În **Profiluri** filă, faceți clic **Setări**.
3. Selectează butonul **Configurează** din zona Profil Joc.
4. Alegeți ajustările sistemului pe care doriți să le aplicați, bifând următoarele opțiuni:
   - Crește performanța jocurilor
   - Optimizează setările de produs pentru Profilul Joc
   - Amânați programele de fundal și sarcinile de întreținere
   - Amânați actualizările automate Windows
   - Ajustează configurările planului de energie pentru jocuri
5. Clic **SALVA** pentru a salva modificările și a închide fereastra.

Adăugare manuală de jocuri la lista de jocuri

În cazul în care Bitdefender nu intră automat în Profilul Joc atunci când ați lansat un anumit joc sau o aplicație, aveți posibilitatea să adăugați aplicația manual la **Lista de aplicații de jocuri**.

Pentru a adăuga manual jocuri în Lista de aplicații de jocuri în Profilul Joc:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Apasă pe **Configurați** butonul din zona Profil de joc.
4. În fereastra **Setări profil joc**, fă clic pe **Lista de jocuri**.
5. Clic **ADĂUGA**.
   Se afișează o nouă fereastră. Mergeți la locația unde se găsește fișierul executabil al jocului, selectați-l și faceți clic pe **OK** pentru a-l adăuga în listă.

Profil Wi-Fi public

Trimiterea de e-mailuri, introducerea unor date de autentificare sensibile sau cumpărăturile online în timp ce sunteți conectat la rețele wireless nesigure pot expune la riscuri datele dumneavoastră personale. Profilul Wi-Fi public ajustează setările produsului pentru a vă da posibilitatea de a face plăți online și de a utiliza informații sensibile într-un mediu protejat.

Configurarea profilului Wi-Fi public

Pentru a configura Bitdefender să aplice setările produsului în timpul conectării la o rețea wireless nesigură:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Faceți clic pe butonul **CONFIGUREAZĂ** din zona Profil Wi-Fi public.
4. Permiteți **să ajusteze setările produsului pentru a optimiza protecția atunci când sunteți conectat la o rețea Wi-Fi publică nesigură căsuța** bifată.
5. Clic **Salvați**.

Profil mod baterie

Modul Baterie se adresează utilizatorilor de laptop si tablete. Scopul este acela de a reduce impactul sistemului și al Bitdefender asupra consumului de electricitate dacă nivelul bateriei este inferior celui implicit sau celui selectat de dumneavoastră.

Configurarea Modului Baterie

Pentru a configura profilul Mod baterie:

1. Clic **Utilități** din meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Selectează butonul **Configurează** din zona Mod Baterie.
4. Selectează ajustările sistemului care vor fi aplicate, prin bifarea opțiunilor de mai jos:
   - Optimizează setările de produs pentru Profilul Baterie.
   - Amână programele de fundal și activitățile de întreținere.
   - Amânare actualizare Windows automată.
   - Ajustează configurările planului de energie pentru Modul Baterie.
   - Dezactivează dispozitivele externe și porturile de rețea.
5. Clic **SALVA** pentru a salva modificările și a închide fereastra.

Introdu o valoare validă în casetă sau selectează una folosind săgețile sus/jos pentru a specifica când să intre sistemul în Modul Baterie. Implicit, modul este activat când nivelul de încărcare a bateriei scade sub 30%.

Când Bitdefender operează în Modul Baterie, se aplică următoarele setări:

- Actualizarea automată Bitdefender este amânată.
- Scanările programate sunt amânate.

Bitdefender detectează dacă laptopul a fost trecut pe alimentarea cu bateire și, în funcție de nivelul de încărcare al bateriei, intră automat în Modul Baterie. De asemenea, Bitdefender iese automat din modul pentru baterie, atunci când detectează că laptopul nu mai funcționează pe baterie.

Optimizare în timp real

Modulul Bitdefender Optimizare în timp real este un plugin care îmbunătățește performanța sistemului în mod silențios, în fundal, asigurându-se că nu ești întrerupt atunci când este activat un profil. În funcție de sarcina înregistrată la nivelul procesorului, pluginul monitorizează toate procesele, concentrându-se pe cele care au o sarcină mai mare, pentru a le ajusta în funcție de nevoile tale.

Pentru a activa sau dezactiva optimizarea în timp real:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Profiluri** filă, faceți clic **Setări**.
3. Derulează în jos până când observi opțiunea de optimizare în timp real și apoi folosește butonul corespunzător pentru a o activa sau dezactiva.

3.3.2. OneClick Optimizer

Probleme precum defecțiunile hard diskului, fișierele de registry rămase și istoricul browserului vă pot încetini activitatea, ceea ce poate deveni sâcâitor pentru dvs. Toate acestea pot fi acum remediate cu un singur clic pe buton.

OneClick Optimizer vă permite să identificați și să eliminați fișierele inutile executând mai multe sarcini de curățare în același timp.

Pentru a începe procesul OneClick Optimizer:

1. Clic **Utilități** din meniul de navigare de pe Interfața Bitdefender.
2. Apasă pe **Optimizați** buton.
   a. **Analizand**
   Așteptați ca Bitdefender să termine căutarea problemelor de sistem.
   - Disk Cleanup - identifică fișierele și folderele inutile.
   - Registry Cleanup - identifică referințe invalide sau învechite în Registry Windows.
   - Curățare confidențialitate - identifică fișierele temporare de internet și cookie-urile, memoria cache a browserului și istoricul.

   Este afișat numărul de probleme găsite. Faceți clic pe linkul Vizualizare detalii pentru a le examina înainte de a continua cu procesul de curățare. Faceți clic pe Optimizare pentru a continua.
   b. **Optimizarea**
   Așteptați ca Bitdefender să termine optimizarea sistemului.
   c. **Probleme**
   Aici puteți vizualiza rezultatul operației.
   Dacă doriți informații complete despre procesul de optimizare, faceți clic pe **Vezi raportul detaliat** buton.

3.3.3. Data Protection

Ștergerea permanentă a fișierelor

Atunci când ștergi un fișier, acesta nu mai poate fi accesat prin metodele obișnuite. Cu toate acestea, fișierul continuă să existe pe hard-disk până ce este suprascris prin copierea altor fișiere.

Bitdefender File Shredder vă ajută să ștergeți definitiv datele eliminându-le fizic de pe hard disk.

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

1. Efectuează clic dreapta pe un fișier sau director pe care dorești să-l ștergi definitiv.

2. Selectează **Bitdefender > Ștergere definitivă fișiere** în meniul contextual afișat.
3. Selectează **Șterge definitiv** și apoi confirmă că dorești să continui procesul.
   Așteptați până când Bitdefender finalizează procesul de ștergere.
4. Sunt afișate rezultatele. Selectează **Finalizare** pentru a părăsi asistentul.

Ca alternativă, poți șterge definitiv fișierele din interfața Bitdefender, după cum urmează:

1. Clic **Utilități** din meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **Protecția datelor**, fă clic pe **Ștergere definitivă fișiere**.
3. Urmează pașii asistentului de ștergere definitivă a fișierelor:
   a. Selectează butonul **Adaugă directoare** pentru a adăuga fișierele sau directoarele pe care dorești să le ștergi definitiv.
      Ca alternativă, glisează aceste fișiere sau foldere în această fereastră.
   b. Selectează **Șterge definitiv** și apoi confirmă că dorești să continui procesul.
      Așteptați ca Bitdefender să termine de distrugere fișierele.
   c. **Sumarul rezultatelor**
      Rezultatele sunt afișate. Clic **finalizarea** pentru a ieși din vrăjitor.

3.4. Cum să

3.4.1. Instalare

Cum instalez Bitdefender pe un al doilea dispozitiv?

Dacă abonamentul achiziționat acoperă mai mult de un dispozitiv, poți utiliza contul tău Bitdefender pentru a activa un al doilea calculator.

Pentru a instala Bitdefender pe un al doilea dispozitiv:

1. Fă clic pe **Instalare pe alt dispozitiv** din colțul din stânga jos al **interfeței Bitdefender**.
   O nouă fereastră apare pe ecran.

2. Clic **SHARE LINK DE DESCARCARE**.
3. Urmează instrucțiunile de pe ecran pentru a instala Bitdefender.

Dispozitivul pe care ați instalat Bitdefender va fi afișat în secțiunea Dispozitivele mele, în Bitdefender Central.

Cum reinstalez Bitdefender?

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

- ai reinstalat sistemul de operare.
- doresc să remediez problemele care este posibil să fi cauzat încetiniri ale proceselor sau căderi de sistem.
- produsul dumneavoastră Bitdefender nu pornește sau nu funcționează corespunzător.

În eventualitatea în care te afli într-una dintre situațiile menționate mai sus, urmează acești pași:

- În **Windows 7**:
  1. Clic **start** și du-te la **Toate programele**.
  2. Găsește Bitdefender Ultimate Small Business Security și selectează **Dezinstalare**.
  3. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată.
  4. După finalizarea procesului, va fi necesară repornirea dispozitivului.
- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
  2. Fă clic pe **Dezinstalare** pentru a dezinstala un program sau **Programe și caracteristici**.
  3. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  4. Clic **REINSTALA** în fereastra care apare.
  5. Trebuie să reporniți dispozitivul pentru a finaliza procesul.

- În **Windows 10** și **Windows 11**:
  1. Fă clic pe **Start**, apoi pe **Setări**.
  2. Fă clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează **Aplicații și caracteristici**.
  3. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
  5. Fă clic pe **REINSTALARE**.
  6. Trebuie să reporniți dispozitivul pentru a finaliza procesul.

> **Notă**
> Urmând această procedură de reinstalare, setările personalizate sunt salvate și vor fi disponibile în noul produs instalat. Celelalte setări pot fi restabilite la configurația implicită.

De unde pot descărca produsul meu Bitdefender?

Poți instala Bitdefender folosind CD-ul de instalare sau aplicația de instalare web pe care o poți descărca pe dispozitivul tău din platforma Bitdefender Central.

> **Notă**
> Înainte de a rula aplicația de instalare, vă recomandăm să dezinstalați orice soluție de securitate de pe sistemul dumneavoastră. Atunci când utilizezi mai multe soluții de securitate pe același dispozitiv, sistemul devine instabil.

Pentru a instala Bitdefender din Bitdefender Central:

1. Acces Bitdefender Central.
2. Selectează **Dispozitivele mele** panou, apoi faceți clic **INSTALATI PROTECTIA**.
3. Alegeți una dintre cele două opțiuni disponibile:
   - **Protejați acest dispozitiv**
     Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.

- **Protejați alte dispozitive**
  Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
  Clic **TRIMITE LINK DE DESCARCARE**. Introduceți o adresă de e-mail în câmpul corespunzător și faceți clic **TRIMITE EMAIL**. Rețineți că linkul de descărcare generat este valabil doar pentru următoarele 24 de ore. Dacă linkul expiră, va trebui să generați unul nou urmând aceiași pași.
  Pe dispozitivul pe care doriți să vă instalați produsul Bitdefender, verificați contul de e-mail pe care l-ați introdus, apoi faceți clic pe butonul de descărcare corespunzător.

4. Rulați produsul Bitdefender descărcat.

Cum folosesc abonamentul Bitdefender după un upgrade Windows?

Această situație apare atunci când faceți un upgrade al sistemului de operare și doriți utilizați în continuare abonamentul Bitdefender.

Dacă utilizezi o versiune Bitdefender anterioară, poți face upgrade gratuit la cea mai nouă versiune Bitdefender, după cum urmează:

- De la versiunea anterioară a Antivirus Bitdefender la cea mai recentă versiune disponibilă a Antivirus Bitdefender.
- De la o versiune anterioară a Bitdefender Internet Security la cea mai recentă versiune disponibilă a Bitdefender Internet Security.
- De la o versiune anterioară a Bitdefender Total Security la cea mai recentă versiune disponibilă a Bitdefender Total Security.

Pot apărea două cazuri:

- Ați făcut upgrade la sistemul de operare folosind Windows Update și ați observat că Bitdefender nu mai funcționează.
  În acest caz, este necesar să reinstalezi produsul urmând acești pași:
  - În **Windows 7**:
    1. Fă clic pe **Start**, accesează **Panoul de control** și fă dublu clic pe **Programe și caracteristici**.

2. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
3. Clic **REINSTALA** în fereastra care apare.
4. Așteaptă finalizarea procesului de dezinstalare și apoi repornește sistemul.
   Deschideți interfața noului produs Bitdefender instalat pentru a avea acces la caracteristicile sale.

- În **Windows 8** și **Windows 8.1**:

1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
2. Fă clic pe **Dezinstalează un program** sau pe **Programe și caracteristici**.
3. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
4. Clic **REINSTALA** în fereastra care apare.
5. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
   Deschideți interfața noului dumneavoastră produs Bitdefender instalat pentru a avea acces la funcțiile acestuia.

- În **Windows 10** și **Windows 11**:

1. Clic **start**, apoi apasa **Setări**.
2. Fă clic pe pictograma **Sistem** din secțiunea Setări, apoi selectează **Aplicații**.
3. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
5. Clic **REINSTALA** în fereastra care apare.
6. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
   Deschideți interfața noului dumneavoastră produs Bitdefender instalat pentru a avea acces la funcțiile acestuia.

Notă
Urmând această procedură de reinstalare, setările personalizate sunt salvate și disponibile în noul produs instalat. Alte setări pot fi comutate înapoi la configurația lor implicită.

- Ați modificat sistemul dumneavoastră și doriți să utilizați în continuare protecția Bitdefender. Prin urmare, trebuie să reinstalați produsul folosind cea mai recentă versiune.
  Pentru a rezolva această problemă:

  1. Descarcă fișierul de instalare:
     a. Acces Bitdefender Central.
     b. Selectează **Dispozitivele mele** panou, apoi faceți clic **INSTALATI PROTECTIA**.
     c. Alegeți una dintre cele două opțiuni disponibile:
        - **Protejați acest dispozitiv**
          Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
        - **Protejează un alt dispozitiv**
          Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
          Clic **TRIMITE LINK DE DESCARCARE**. Introduceți o adresă de e-mail în câmpul corespunzător și faceți clic **TRIMITE EMAIL**. Rețineți că linkul de descărcare generat este valabil doar pentru următoarele 24 de ore. Dacă linkul expiră, va trebui să generați unul nou urmând aceiași pași.
          Pe dispozitivul pe care doriți să vă instalați produsul Bitdefender, verificați contul de e-mail pe care l-ați introdus, apoi faceți clic pe butonul de descărcare corespunzător.

  2. Rulați produsul Bitdefender pe care l-ați descărcat.

  Pentru mai multe informații cu privire la procesul de instalare Bitdefender, consultați Instalarea produsului dumneavoastră Bitdefender (pagina 11).

Cum pot face upgrade la cea mai recentă versiune Bitdefender?

De acum înainte, actualizarea la cea mai recentă versiune este posibilă fără a urma procedura de dezinstalare și reinstalare manuală. Mai exact, noul produs care include noi caracteristici și îmbunătățiri majore de produs este livrat prin intermediul actualizărilor de produs și, dacă aveți deja un abonament Bitdefender activ, produsul se activează automat.

Dacă folosești versiunea 2020, poți face upgrade la cea mai nouă versiune urmând acești pași:

1. Efectuați clic pe **REPORNEȘTE ACUM** în fereastra de notificare în care sunt afișate informațiile privind actualizarea. Dacă ați ratat-o, accesați fereastra **Notificări**, identificați cea mai recentă actualizare și apoi efectuați clic pe butonul **REPORNEȘTE ACUM**. Așteaptă ca dispozitivul să repornească.
   Se va afișa fereastra **Ce este nou** conținând informațiile despre caracteristicile noi și îmbunătățite.
2. Efectuați clic pe link-urile **Citiți mai multe** pentru redirectare către pagina noastră dedicată conținând mai multe detalii și articole utile.
3. Închideți fereastra **Ce este nou** pentru a accesa interfața noi versiuni instalate.

Utilizatorii care doresc să facă upgrade gratuit de la Bitdefender 2016 sau o versiune anterioară la cea mai recentă versiune a Bitdefender trebuie să dezinstaleze versiunea lor actuală din Panoul de control și apoi să descarce cel mai recent fișier de instalare de pe site-ul Bitdefender accesând următoarea adresă: https://www.bitdefender.com/Downloads/. Activarea este posibilă doar cu un abonament valid.

3.4.2. Bitdefender Central

Cum mă pot conecta la contul Bitdefender cu un alt cont?

Ai creat un cont Bitdefender nou și vrei să-l utilizezi pe acesta de acum încolo.

Pentru a vă autentifica cu alt cont Bitdefender:

1. Selectează numele contului tău în partea superioară a interfeței **Bitdefender**.

2. Selectează **Schimbă contul** din colțul din dreapta sus al ecranului pentru a schimba contul asociat dispoztivului respectiv.
3. Tastați adresa de e-mail în câmpul corespunzător, apoi faceți clic **URMĂTORUL**.
4. Introduceți parola, apoi faceți clic **CONECTARE**.

> **Notă**
> Produsul Bitdefender de pe dispozitivul tău se schimbă automat în funcție de abonamentul asociat noului cont Bitdefender. Dacă nu există niciun abonament disponibil asociat noului cont Bitdefender sau dacă vrei să transferi abonamentul din contul anterior, poți contacta Bitdefender pentru asistență așa cum se descrie în secțiunea Solicitarea ajutorului (pagina 290).

Cum dezactivez mesajele de asistență Bitdefender Central?

Pentru a te ajuta să înțelegi cum să folosești fiecare opțiune din Bitdefender Central, în panoul de bord sunt afișate mesaje de ajutor.

Dacă dorești să nu mai vezi acest tip de mesaje:

1. Acces Bitdefender Central.
2. Apasă pe pictograma din partea dreaptă sus a ecranului.
3. Fă clic pe **Contul meu** în meniul derulant.
4. Selectează opțiunea **Setări** din meniul derulant.
5. Dezactivează opțiunea **Activează/Dezactivează mesajele de ajutor**.

Am uitat parola setată pentru contul meu Bitdefender. Cum se resetează?

Există două posibilități pentru a seta o nouă parolă pentru contul dumneavoastră Bitdefender:

- De la Interfața Bitdefender:
  1. Clic **Contul meu** pe meniul de navigare de pe Interfața Bitdefender.
  2. Selectează {1}Schimbă contul{2} din colțul din dreapta sus al ecranului.
     Se afișează o nouă fereastră.
  3. Introdu adresa ta de e-mail și selectează {1}ÎNAINTE{2}.

Apare o nouă fereastră.

4. Clic **Ați uitat parola?**.
5. Apasă pe {1}ÎNAINTE{2}.
6. Verificați-vă contul de e-mail, introduceți codul de securitate pe care l-ați primit, apoi faceți clic **URMĂTORUL**.
   Alternativ, puteți face clic **Schimbați parola** în e-mailul pe care ți l-am trimis.
7. Introduceți noua parolă pe care doriți să o setați, apoi introduceți-o din nou. Clic **SALVA**.

❍ Din browserul dvs. web:

1. Mergi la: https://central.bitdefender.com.
2. Fă clic pe {1}CONECTARE{2}.
3. Introduceți adresa dvs. de e-mail, apoi faceți clic **URMĂTORUL**.
4. Clic **Ați uitat parola?**.
5. Clic **URMĂTORUL**.
6. Verifică-ți contul de e-mail și urmărește instrucțiunile furnizate pentru a seta o nouă parolă pentru contul tău Bitdefender.

Pentru a accesa ulterior contul Bitdefender, introduceți adresa e-mail și noua parolă setată.

Cum pot gestiona sesiunile de autentificare asociate contului meu Bitdefender?

În contul dumneavoastră Bitdefender, aveți posibilitatea de a vizualiza cele mai recente sesiuni de autentificare active și inactive de pe dispozitivele asociate contului dumneavoastră. În plus, vă puteți deconecta de la distanță urmând acești pași:

1. Acces Bitdefender Central.
2. Apasă pe pictograma din partea dreaptă sus a ecranului.
3. Selectează **Sesiuni** din meniul derulant.
4. În secțiunea **Sesiuni active**, selectează opțiunea **DECONECTARE** din dreptul dispozitivului pe care dorești să închei sesiunea.

3.4.3. Scanarea cu BitDefender

Cum scanez un fișier sau un director?

Cea mai ușoară metodă de a scana un fișier sau un director este să faci clic dreapta pe un obiect pe care dorești să-l scanezi, să alegi Bitdefender și să selectezi **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, ți se va cere să selectezi acțiunile ce vor fi aplicate în cazul acestora.

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

- Suspectezi un anumit fișier sau director că este infectat.
- Atunci când descarci fișiere de pe internet considerate că ar putea fi periculoase.
- Scanează un director comun din rețea înainte de a copia fișiere din acesta pe dispozitivul tău.

Cum îmi scanez sistemul

Pentru a realiza o scanare completă a sistemului:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Fă clic pe butonul **Rulează scanare** din dreptul **Scanare sistem**.
4. Urmați programul asistent Scanare Sistem pentru a încheia 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, consultă capitolul .

Cum programez o scanare?

Poți configura Bitdefender să activeze scanarea locațiilor importante de sistem când nu te afli la dispozitiv.

Pentru a programa o scanare:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Selectează ··· de lângă tipul scanării pe care vrei să o programezi, Scanare sistem sau Scanare rapidă, în partea inferioară a interfeței, apoi selectează **Editare**.
   Ca metodă alternativă, poți crea un tip de scanare care să corespundă necesităților tale selectând **+Creare scanare** din dreptul **Administrare scanări**.
4. Personalizează scanarea în funcție de nevoile tale, apoi selectează **Înainte**.
5. Bifează caseta de lângă **Alege când vei programa această sarcină**.
   Selectează una dintre opțiunile corespunzătoare pentru a seta un program:
   - La pornirea sistemului
   - Zilnic
   - Săptămânal
   - Lunar

   Dacă alegeți Zilnic, Lunar sau Săptămânal, trageți glisorul de-a lungul scalei pentru a seta perioada dorită de timp în care ar trebui să înceapă scanarea programată.

Dacă alegi să creezi o nouă scanare personalizată, se va afișa fereastra **Sarcină de scanare**. De aici poți selecta locațiile care dorești să fie scanate.

Cum creez o activitate de scanare personalizată?

Dacă dorești să scanezi anumite locații de pe dispozitiv sau pentru a configura opțiunile de scanare, poți configura și rula o sarcină de scanare personalizată.

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

1. În **ANTIVIRUS** panou, faceți clic **Deschis**.
2. Fă clic pe **+Creare scanare** din dreptul **Administrare scanări**.

3. În câmpul Nume sarcină, introdu o denumire pentru scanarea respectivă, apoi selectează locațiile care dorești să fie scanate și selectează **ÎNAINTE**.
4. Configurați aceste opțiuni generale:
   - **Scanează numai aplicații.** Poți configura Bitdefender să scaneze doar aplicațiile accesate.
   - **Prioritate scanare sarcină.** Poți alege ce impact ar trebui să aibă un proces de scanare asupra performanței sistemului tău.
     - Auto - Prioritatea procesului de scanare va depinde de activitatea sistemului. Pentru a se asigura că procesul de scanare nu va afecta activitatea sistemului, Bitdefender va decide dacă procesul de scanare ar trebui să fie rulat cu prioritate mare sau scăzută.
     - High - Prioritatea procesului de scanare va fi mare. Alegând această opțiune, veți permite altor programe să ruleze mai lent și veți reduce timpul necesar pentru finalizarea procesului de scanare.
     - Scăzută - Prioritatea procesului de scanare va fi scăzută. Alegând această opțiune, veți permite altor programe să ruleze mai rapid și veți crește timpul necesar pentru finalizarea procesului de scanare.
   - **Acțiuni post-scanare.** Alege ce acțiune ar trebuie să implementeze Bitdefender în cazul în care nu sunt identificate amenințări:
     - Afișează fereastra Rezumat
     - Dispozitiv de oprire
     - Închideți fereastra Scanare
5. Dacă dorești să configurezi în detaliu opțiunile de scanare, selectează **Afișează opțiuni avansate**.
   Clic **Următorul**.
6. Dacă dorești, poți activa opțiunea **Programează sarcina de scanare** și apoi poți alege când ar trebui să pornească sarcina personalizată pe care ai creat-o.
   - La pornirea sistemului

- Zilnic
- Lunar
- Săptămânal

Dacă alegeți Zilnic, Lunar sau Săptămânal, trageți glisorul de-a lungul scalei pentru a seta perioada dorită de timp în care ar trebui să înceapă scanarea programată.

7. Clic **Salvați** pentru a salva setările și a închide fereastra de configurare.
   În funcție de locațiile care urmează să fie scanate, scanarea poate dura ceva timp. Dacă în timpul procesului de scanare vor fi găsite amenințări, vi se va solicita să alegeți acțiunile care trebuie întreprinse asupra fișierelor detectate.

Dacă dorești, poți relua rapid rularea scanării personalizate anterioare, făcând clic pe înregistrarea corespunzătoare din lista valabilă.

Cum exclud un director de la procesul de scanare?

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

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

- Ai un director mare pe sistemul tău în care există filme și muzică
- Ai o arhivă mare pe sistemul tău în care păstrezi 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 un director în lista de Excepții:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Fă clic pe fila **Setări**.
4. Fă clic pe **Gestionare excepții**.
5. Clic **+ Adăugați o excepție**.
6. Introduceți calea folderului pe care doriți să-l faceți, cu excepția scanării, în câmpul corespunzător.

Alternativ, puteți naviga la folder făcând clic pe butonul de răsfoire din partea dreaptă a interfeței, selectați-l și faceți clic pe **Bine**.

7. Porniți comutatorul de lângă caracteristica de protecție care nu ar trebui să scaneze folderul. Există trei opțiuni:
   - Antivirus
   - Prevenirea amenințărilor online
   - Apărare avansată împotriva amenințărilor
8. Clic **Salvați** pentru a salva modificările și a închide fereastra.

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

Pot exista situații în care Bitdefender marchează greșit un fișier legitim ca fiind o amenințare (un rezultat fals pozitiv). Pentru a corecta această eroare, adaugă fișierul în secțiunea de excepții:

1. Dezactivează protecția antivirus în timp real a Bitdefender:
   a. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
   b. În **ANTIVIRUS** panou, faceți clic **Deschis**.
   c. În fereastra **Setări avansate**, dezactivează **Scutul Bitdefender**.
   Se deschide 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 de minute, pentru o oră, permanent sau doar până la repornirea sistemului.
2. Afișează obiecte ascunse în Windows. Pentru a afla cum să faci acest Cum pot afișa elementele ascunse din Windows? (pagina 119)lucru, consultă .
3. Restaurează fișierul din zona de carantină:
   a. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
   b. În **ANTIVIRUS** panou, faceți clic **Deschis**.
   c. Accesează ferestrele **Setări** și fă clic pe **Administrare carantină**.
   d. Selectează fișierul și apoi fă clic pe **Restabilire**.

4. Adaugă fișierul în lista de excepții. Pentru a afla cum să faci acest lucru, consultă Cum exclud un director de la procesul de scanare? (pagina 106).
5. Activați protecția antivirus în timp real a Bitdefender.
6. Contactează un reprezentant al echipei noastre de asistență tehnică și solicită eliminarea mesajului de informare privind amenințările. Pentru a afla cum să faci acest lucru, consultă Solicitarea ajutorului (pagina 290).

Cum aflu ce amenințări au fost detectate 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 jurnalul de scanare direct din expertul de scanare, odată ce scanarea este finalizată, făcând clic **ARATĂ JURNAL**.

Pentru a verifica mai târziu un jurnal de scanare sau orice infecție detectată:

1. Clic **Notificări** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Toate** fila, selectați notificarea privind cea mai recentă scanare.
   Aici puteți găsi toate evenimentele de scanare a amenințărilor, inclusiv amenințările detectate prin scanarea la acces, scanările inițiate de utilizator și modificările de stare pentru scanările automate.
3. În lista de notificări, puteți verifica ce scanări au fost efectuate recent. Faceți clic pe o notificare pentru a vedea detalii despre aceasta.
4. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**.

3.4.4. Control date personale

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, proiectat pentru a-ți proteja informațiile privind cardurile bancare, numărul de cont sau orice alte date confidențiale pe care le-ai introdus atunci când accesezi diferite locații online.

Pentru a menține securitatea și confidențialitatea activității tale online:

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
2. În **SAFEPAY** panou, faceți clic **Setări**.
3. În **Safepay** fereastra, faceți clic **Lansați Safepay**.
4. Fă clic pe butonul pentru a accesa **Tastatura virtuală**.
   Folosiți **Tastatura virtuală** atunci când introduceți informații confidențiale, cum ar fi parolele.

Ce pot face dacă mi-a fost furat dispozitivul?

Furtul de dispozitive mobile - indiferent dacă este vorba despre un smartphone, o tabletă sau un laptop - este una dintre principalele probleme care afectează în prezent indivizii și organizațiile din întreaga lume.

Bitdefender Anti-Theft îți permite nu numai să localizezi și să blochezi dispozitivul furat, dar și să ștergi toate datele pentru a te asigura că acestea nu vor fi folosite de autorii furtului.

Pentru a accesa caracteristicile Anti-Theft din contul tău:

1. Acces Bitdefender Central.
2. Selectează **Dispozitivele mele** panou.
3. Efectuează clic pe fila dispozitivului dorit și selectează **Antifurt**.
4. Selectează funcția pe care dorești să o folosești:
   - **LOCALIZARE** - afișează locația dispozitivului dumneavoastră pe Google Maps.
     Afișează IP - afișează ultima adresă IP a dispozitivului selectat.
   - **Alertă** - trimite o alertă pe dispozitiv.
   - **Blocare** - blochează-ți dispozitivul și setează un cod PIN numeric pentru a-l debloca. De asemenea, poți activa o opțiune

corespunzătoare care îi permite Bitdefender să facă fotografii instantanee ale persoanei care încearcă să-ți acceseze dispozitivul.

- **Ștergere** - șterge toate datele din dispozitivul tău.

> **Important**
> După ce ștergi un dispozitiv, este oprită funcționarea tuturor funcțiilor Anti-Theft.

Cum șterg definitiv un fișier cu ajutorul Bitdefender?

Dacă dorești să ștergi definitiv un fișier din sistemul tău, este necesar să ștergi fizic datele de pe hard disk.

Funcția Ștergere definitivă fișiere a Bitdefender te va ajuta să ștergi rapid fișiere sau directoare din dispozitivul tău prin accesarea 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. Clic **Sterge Permanent**, apoi confirmați că doriți să continuați procesul.
   Așteptați ca Bitdefender să termine de distrugere fișierele.
3. Sunt afișate rezultatele. Efectuați clic pe **Finalizare** pentru a părăsi asistentul.

Cum îmi protejez de hackeri camera web?

Puteți configura produsul Bitdefender pentru a permite sau bloca accesul aplicațiilor instalate la camera web urmând acești pași:

1. Clic **Confidențialitate** pe meniul de navigare de pe Interfața Bitdefender.
2. În **PROTECTIE VIDEO & AUDIO** panou, faceți clic **Setări**.
3. Mergi la fereastra {1}Protecția cameră web{2} și vei vedea lista cu aplicațiile care au solicitat accesul la camera ta.
4. Îndreaptă cursorul spre aplicația căreia vrei să îi permiți sau să îi blochezi accesul și apoi selectează butonul reprezentat printr-o cameră video care se află lângă aceasta.
   Pentru a vizualiza opțiunile alese de alți utilizatori Bitdefender în legătură cu aplicația selectată, apasă pe pictograma {1}{2}{3}{4}{5}{6}.

Vei fi notificat de fiecare dată când aplicațiile selectate sunt blocate de utilizatori Bitdefender.

Pentru a adăuga manual aplicații în această listă selectează butonul {1}Adaugă aplicație{2} și apoi selectează una dintre cele două opțiuni.

- Din Windows Store
- Dintre aplicațiile tale

Cum pot restabili manual fișierele criptate atunci când procesul de restabilire eșuează?

În cazul în care fișierele criptat nu pot fi restabilite automat, le poți restabili manual urmând acești pași:

1. Clic **Notificări** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Toate** fila, selectați notificarea cu privire la cel mai recent comportament ransomware detectat, apoi faceți clic **Fișiere criptate**.
3. Se afișează lista cu fișierele criptate.
   Selectează **Recuperare fișiere** pentru a continua.
4. În cazul în care întregul sau o parte a procesului de restaurare eșuează, trebuie să alegeți locația în care ar trebui să fie salvate fișierele decriptate. Clic **Restaurați locația**, apoi alegeți o locație pe computer.
5. Apare o fereastră de confirmare.
   Clic **finalizarea** pentru a încheia procesul de restaurare.

Fișierele cu următoarele extensii pot fi restaurate în cazul în care sunt criptate:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com ; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .ph p; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wa v; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

3.4.5. Instrumente de optimizare

Cum îmi îmbunătățesc performanța sistemului?

Performanța sistemului depinde nu numai de configurația hardware, cum ar fi încărcarea procesorului, utilizarea memoriei și spațiul pe hard disk. De asemenea, este conectat direct la configurația software-ului și la gestionarea datelor.

Acestea sunt principalele acțiuni pe care le puteți face cu Bitdefender pentru a îmbunătăți viteza și performanța sistemului dvs.:

- ❍ Optimizați-vă performanța sistemului cu un singur clic (pagina 112)
- ❍ Scanați-vă sistemul periodic (pagina 112)

Optimizați-vă performanța sistemului cu un singur clic

Opțiunea OneClick Optimizer vă economisește timp prețios atunci când doriți o modalitate rapidă de a vă îmbunătăți performanța sistemului prin scanarea, detectarea și curățarea rapidă a fișierelor inutile.

Pentru a începe procesul OneClick Optimizer:

1. Clic **Utilități** pe meniul de navigare de pe Interfața Bitdefender.
2. Apasă pe **Optimizați** buton.
3. Lăsați Bitdefender să caute fișiere care pot fi șterse, apoi faceți clic pe **Optimizați** butonul pentru a finaliza procesul.

Scanați-vă sistemul periodic

Viteza sistemului și comportamentul său general pot fi, de asemenea, afectate de amenințări.

Asigurați-vă că vă scanați sistemul periodic, cel puțin o dată pe săptămână.

Este recomandat să utilizați Scanarea sistemului deoarece scanează pentru toate tipurile de amenințări care pun în pericol securitatea sistemului dvs. și, de asemenea, scanează în interiorul arhivelor.

Pentru a începe scanarea sistemului:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.

3. Clic **Rulați Scanarea** chiar lângă **Scanarea sistemului**.
4. Urmați pașii vrăjitorului.

3.4.6. Informații utile

Cum îmi testez soluția de securitate?

Pentru a vă asigura că produsul Bitdefender funcționează corespunzător, vă recomandăm să utilizați testul Eicar.

Testul Eicar îți permite să îți verifici soluția de securitate folosind un fișier de siguranță conceput special pentru acest scop.

Pentru a testa soluția de securitate:

1. Descarcă testul de pe pagina web oficială a organizației EICAR http://www.eicar.org/.
2. Faceți clic pe fila **Fișier de testare anti-malware**.
3. Faceți clic pe **Descărcare** în meniul din stânga.
4. Din zona de **Descărcare folosind protocolul standard http** fă clic pe fișierul de testare **eicar.com**.
5. Vei primi notificarea că pagina pe care încerci să o accesezi conține fișierul de testare EICAR (și nu o amenințare).
   Dacă faceți clic pe **Înțeleg riscurile, vreau să continui oricum**, descărcarea pachetului de testare va începe automat și o fereastră pop-up Bitdefender vă va informa că a fost detectată o amenințare.
   Faceți clic pe **Mai multe detalii** pentru a afla mai multe informații despre această acțiune.

Dacă nu primiți nicio alertă Bitdefender, vă recomandăm să contactați Bitdefender pentru asistență, așa cum este indicat la secțiunea Solicitarea ajutorului (pagina 290).

Cum să dezinstalati Bitdefender

Dacă vrei să elimini Bitdefender Ultimate Small Business Security:

❍ În **Windows 7**:

1. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.

2. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
3. Efectuați clic pe **ȘTERGE** în fereastra care se deschide.
4. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
  2. Clic **Dezinstalează un program** sau **Programe si caracteristici**.
  3. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  4. Clic **ELIMINA** în fereastra care apare.
  5. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 10** și **Windows 11**:
  1. Faceți clic pe **Start**, apoi pe Setări.
  2. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații**.
  3. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
  5. Clic **ELIMINA** în fereastra care apare.
  6. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

> **Notă**
> Această procedură de reinstalare va șterge definitiv setările personalizate.

Cum să dezinstalati Bitdefender VPN

Procedura de dezinstalare a aplicației Bitdefender VPN este similară celei utilizate pentru eliminarea altor programe din dispozitivul tău:

- În **Windows 7**:
  1. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
  2. Găsește **Bitdefender VPN** și selectează **Dezinstalare**.
     Așteaptă până când procesul de dezinstalare este finalizat.
- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
  2. Clic **Dezinstalează** un program sau **Programe si caracteristici**.
  3. Găsi **Bitdefender VPN** și selectați **Dezinstalează**.
     Așteptați finalizarea procesului de dezinstalare.
- În **Windows 10** și **Windows 11**:
  1. Clic **start**, apoi faceți clic pe Setări.
  2. Fă clic pe pictograma **Sistem** din secțiunea Setărilor, apoi selectează **Aplicații instalate**.
  3. Găsi **Bitdefender VPN** și selectați **Dezinstalează**.
  4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
     Așteptați finalizarea procesului de dezinstalare.

Cum dezinstalez extensia Bitdefender Anti-tracker?

În funcție de browserul web pe care îl utilizezi, urmează acești pași pentru a dezinstala extensia Bitdefender Anti-tracker:

- Internet Explorer
  1. Fă clic pe de lângă bara de căutare, apoi selectează Gestionare add-on. Se afișează lista extensiilor instalate.
  2. Fă clic pe Bitdefender Anti-tracker.
  3. Selectează **Dezactivare** din dreapta jos.
- Google Chrome
  1. Fă clic pe ⋮ din dreptul barei de căutare.

2. Selectează **Mai multe instrumente** și apoi **Extensii**.
   Se va afișa o listă cu extensiile instalate.
3. Apasă pe **Eliminare** în căsuța Bitdefender Anti-tracker card.
4. Selectează opțiunea **Dezinstalează** din fereastra care se deschide.

❍ Mozilla Firefox

1. Clic ≡ lângă bara de căutare.
2. Selectează **Add-on** și apoi **Extensii**.
   Apare o listă cu extensiile instalate.
3. Fă clic pe ⋯ și apoi selectează **Eliminare**.

Cum închid automat dispozitivul 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 amenințări. Scanarea întregului dispozitiv poate dura destul de mult timp, în funcție de configurația hardware și software a sistemului tău.

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

Spre exemplu: ți-ai terminat treaba și vrei să mergi la culcare. Doriți să efectuați o verificare integrală a sistemului dumneavoastră în vederea detectării amenințărilor cu ajutorulBitdefender.

Pentru a opri dispozitivul în momentul finalizării unei sarcini de Scanare rapidă sau Scanare de sistem:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. În fereastra **Scanări**, fă clic pe ⋯ din dreptul opțiunii Scanare rapidă sau Scanare sistem și apoi selectează **Editare**.
4. Personalizează scanarea în funcție de nevoile tale, apoi selectează **Înainte**.
5. Bifează caseta de lângă **Alege când vei programa această sarcină** și apoi alege când va începe această sarcină.

Dacă alegeți Zilnic, Lunar sau Săptămânal, trageți glisorul de-a lungul scalei pentru a seta perioada dorită de timp în care ar trebui să înceapă scanarea programată.

6. Clic **Salvați**.

Pentru a închide dispozitivul după finalizarea scanării personalizate:

1. Apasă pe ··· din dreptul opțiunii de scanare personalizată pe care ai creat-o.
2. Fă clic pe **Înainte** și apoi pe **Înainte** din nou.
3. Bifează caseta de lângă **Alege când vei programa această sarcină** și apoi alege când va începe această sarcină.
4. Clic **Salvați**.

Dacă nu este detectată nicio amenințare, dispozitivul 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, consultă capitolul Asistentul de scanare antivirus (pagina 30).

Cum configurez Bitdefender să utilizeze o conexiune de internet prin proxy?

Dacă dispozitivul tău se conectează la internet prin intermediul unui server proxy, trebuie să configurezi 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 administra setările proxy:

1. Clic **Setări** pe meniul de navigare de pe Interfața Bitdefender.
2. Selectează **Avansat** fila.
3. Activează **Server proxy**.

4. Fă clic pe **Schimbă proxy**.
5. 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, 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 de Microsoft Edge,Internet Explorer, Mozilla Firefox și Google Chrome.

   - **Setări proxy personalizate** - setări proxy pe care le puteți configura cum doriți.
     Următoarele setări trebuie specificate:
     - **Adresă** - tastează IP-ul serverului proxy.
     - **Port** - introdu portul utilizat de Bitdefender pentru a se conecta la serverul proxy.
     - **Nume de utilizator** - introdu numele de utilizator recunoscut de proxy.
     - **Parola** - introdu parola validă a utilizatorului anterior.
6. 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.

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

Pentru a afla dacă ai un sistem de operare pe 32 sau 64 de biți:

- În **Windows 7**:
  1. Fă clic pe **Start**.
  2. Găsește **Computer** în meniul **Start**.
  3. Fă clic dreapta pe **Computer** și apoi selectează **Proprietăți**.
  4. Sub **System** veți găsi informații referitoare la sistemul dumneavoastră.

- În **Windows 8**:
  1. Din ecranul de Start al Windows, localizați **Computer** (de exemplu, puteți începe să tastați „Computer” direct în ecranul de Start) și faceți clic dreapta pe pictograma acestuia.
  2. Selectează **Proprietăți** din meniul din partea de jos.
  3. Mergi la secțiunea Sistem pentru a vedea tipul sistemului.
- În **Windows 10** și **Windows 11**:
  1. Introdu "System" în caseta de căutare din bara de sarcini și efectuează clic pe pictogramă.
  2. Caută în zona System pentru a afla informații referitoare la tipul de sistem.

Cum pot afișa elementele ascunse din Windows?

Acești pași sunt utili în acele cazuri în care ai de-a face cu o situație în care este implicată o amenințare și trebuie să găsesti și să elimini fișierele infectate, care pot fi ascunse.

Urmează acești pași pentru a afișa obiectele ascunse din Windows:

1. Fă clic pe **Start**, mergi la **Panoul de control**.
   În **Windows 8** și **Windows 8.1**: din ecranul de Start al Windows, găsește **Panoul de control** (de exemplu, poți începe să tastezi „Control panel/Panoul de control” direct în ecranul de Start) și fă clic pe pictograma acestuia.
2. Selectează **Opțiuni director**.
3. Mergi la fila **Vizualizare**.
4. Selectați **Show hidden files and folders**.
5. Debifați **Hide extensions for known file types**.
6. Debifați **Hide protected operating system files**.
7. Fă clic pe **Aplică**, apoi pe **OK**.

În **Windows 10** și **Windows 11**:

1. Introdu "Show hidden files and folders" în caseta de căutare din bara de sarcini și efectuează clic pe pictogramă.

2. Selectați **Show hidden files, folders, and drives**.
3. clar **Ascunde extensiile pentru tipurile de fișiere cunoscute**.
4. clar **Ascundeți fișierele protejate ale sistemului de operare**.
5. Clic **aplica**, apoi apasa **Bine**.

Cum elimin celelalte 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 utilizezi mai multe soluții de securitate pe același dispozitiv, sistemul devine instabil. Programul de instalare al Bitdefender Ultimate Small Business Security detectează în mod automat alte programe de securitate și vă oferă opțiunea de a le dezinstala.

Dacă nu ai dezinstalat celelalte soluții de securitate în timpul instalării inițiale:

- În **Windows 7**:
  1. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
  2. Așteaptă câteva momente până când este afișată lista programelor instalate.
  3. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Dezinstalare**.
  4. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
  2. Clic **Dezinstalați un program** sau **Programe si caracteristici**.
  3. Așteptați câteva momente până când este afișată lista de software instalat.

4. Găsiți numele programului pe care doriți să îl eliminați și selectați **Dezinstalează**.
5. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 10** și **Windows 11**:
  1. Clic **start**, apoi faceți clic pe Setări.
  2. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații**.
  3. Găsiți numele programului pe care doriți să îl eliminați și selectați **Dezinstalează**.
  4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
  5. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

Dacă nu reușești să elimini cealaltă soluție de securitate, descarcă instrumentul de dezinstalare de pe site-ul furnizorului sau contactează-l direct pentru a-ți oferi instrucțiuni cu privire la dezinstalare.

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 amenințările 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 amenințărilor sunt inactive atunci când Windows se află în Safe Mode și pot fi eliminate cu ușurință.

Pentru a porni Windows în Safe Mode:

- În **Windows 7**:
  1. Repornește dispozitivul
  2. Apăsați tasta **F8** de mai multe ori înainte ca Windows să pornească pentru a avea acces la meniul de pornire.

3. Selectează **Safe Mode** (Mod de siguranță) în meniul de pornire sau **Safe Mode with Networking** (Mod de siguranță cu rețea) dacă dorești să ai acces la internet.
4. Apăsați **Enter** și așteptați până când Windows se încarcă în Safe Mode.
5. Acest proces este finalizat cu un mesaj de confirmare. Apasă pe **OK** pentru a confirma.
6. Pentru a porni Windows în mod normal, repornește pur și simplu sistemul.

- În **Windows 8**, **Windows 8.1**, **Windows 10** și **Windows 11**:
  1. Lansează aplicația **System Configuration** (Configurație sistem) din Windows apăsând simultan tastele **Windows + R**.
  2. Introdu **msconfig** în caseta de dialog **Open** (Deschide) apoi apasă pe **OK**.
  3. Selectează fila **Boot** (Pornire).
  4. În secțiunea **Boot options** (Opțiuni pornire), bifează caseta **Safe boot** (Pornire în mod de siguranță).
  5. Fă clic pe **Network** (Rețea) și apoi pe **OK**.
  6. Fă clic pe **OK** în fereastra **System Configuration** (Configurare sistem) care te informează că sistemul trebuie repornit pentru ca modificările să poată fi implementate.
     Sistemul tău este în curs de repornire în Safe Mode with Networking.

Pentru a reporni dispozitivul în modul normal, modifică din nou setările lansând **System Operation** (Operațiune sistem) și debifând **Safe boot** (Pornire în mod de siguranță). Fă clic pe **OK** și apoi pe **Restart** (Repornire). Așteaptă ca noile setări să fie aplicate.

3.5. Remedierea problemelor

3.5.1. Soluționarea problemelor frecvente

Acest capitol prezintă unele probleme care pot apărea atunci când folosiți BitDefender și vă oferă soluții posibile. Majoritatea acestor probleme pot fi remediate prin configurarea adecvată a setărilor de produs.

Dacă problema dvs nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic BitDefender folosind informațiile din capitolul {1}{2}.

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 observi o încetinire semnificativă, această problemă poate apărea din următoarele motive:

- **Bitdefender nu este singurul program de securitate instalat pe sistem.**
  Deși Bitdefender caută și dezinstalează programele de securitate detectate în timpul instalării, se recomandă să îndepărtați orice alte soluții de securitate pe care le-ați utilizat înainte de a iniția instalarea Bitdefender. Pentru mai multe informații, consultă capitolul Cum elimin celelalte soluții de securitate? (pagina 120).

- **Cerințele de sistem pentru rularea Bitdefender nu sunt îndeplinite.**
  Dacă dispozitivul tău nu îndeplinește cerințele de sistem, dispozitivul va fi afectat de încetiniri, mai ales atunci când mai multe aplicații

rulează în același timp. Pentru mai multe informații, consultă capitolul Cerințe de sistem (pagina 9).

- **Ai instalat aplicații pe care nu le utilizezi.**
  Orice dispozitiv are programe sau aplicații pe care nu le folosești. Și multe programe nedorite rulează în fundal, ocupând spațiu pe disc și încărcând memoria calculatorului. Dacă nu folosiți un program, dezinstalați-l. Acest lucru este valabil și pentru orice alte programe software sau aplicații de evaluare pe care omiteți să le ștergeți.

  > **Important**
  > Dacă suspectezi că un program sau o aplicație este o componentă esențială a sistemului tău de operare, nu le dezinstala, ci contactează Serviciul de asistență clienți al Bitdefender.

- **Sistemul dumneavoastră poate fi infectat.**
  Viteza cu care funcționează sistemul tău și comportamentul general al acestuia pot fi afectate și de amenințări. Programele precum spyware, malware, troieni și adware generează un impact asupra performanței dispozitivului tău. Asigură-te că scanezi periodic sistemul, cel puțin o dată pe săptămână. Se recomandă să utilizezi Bitdefender System Scan pentru că scanează toate tipurile de amenințări care pun în pericol securitatea sistemului tău.
  Pentru a porni Scanarea sistemului:

  1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
  2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
  3. În fereastra **Scanări**, fă clic pe **Efectuează scanare** de lângă **Scanare sistem**.
  4. Urmează pașii asistentului.

Nu începe scanarea

Acest tip de problemă poate avea două cauze principale:

- {1}O instalare anterioară a Bitdefender care nu a fost complet eliminată sau o instalare necorespunzătoare a Bitdefender.{2}
  În acest caz, reinstalează Bitdefender:
  - În **Windows 7**:

1. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
2. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
3. Clic **REINSTALA** în fereastra care apare.
4. Așteaptă finalizarea procesului de reinstalare și apoi repornește sistemul.

- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
  2. Clic **Dezinstalează** un program sau **Programe si caracteristici**.
  3. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  4. Clic **REINSTALA** în fereastra care apare.
  5. Așteptați finalizarea procesului de reinstalare, apoi reporniți sistemul.

- În **Windows 10** și **Windows 11**:
  1. Clic **start**, apoi apasa **Setări**.
  2. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații instalate**.
  3. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
  5. Clic **REINSTALA** în fereastra care apare.
  6. Așteptați finalizarea procesului de reinstalare, apoi reporniți sistemul.

> **Notă**
> Urmând această procedură de reinstalare, setările personalizate sunt salvate și disponibile în noul produs instalat. Alte setări pot fi comutate înapoi la configurația lor implicită.

- **Bitdefender nu este singura soluție de securitate instalată pe sistemul tău.**
  În acest caz:

  1. Dezinstalați cealaltă soluție de securitate. Pentru mai multe informații, consultă capitolul Cum elimin celelalte soluții de securitate? (pagina 120).
  2. Reinstalare Bitdefender:
     - În **Windows 7**:
       a. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
       b. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
       c. Clic **REINSTALA** în fereastra care apare.
       d. Așteptați finalizarea procesului de reinstalare, apoi reporniți sistemul.
     - În **Windows 8** și **Windows 8.1**:
       a. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
       b. Clic **Dezinstalează** un program sau **Programe si caracteristici**.
       c. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
       d. Clic **REINSTALA** în fereastra care apare.
       e. Așteptați finalizarea procesului de reinstalare, apoi reporniți sistemul.
     - În **Windows 10** și **Windows 11**:

a. Clic **start**, apoi apasa **Setări**.

b. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații instalate**.

c. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.

d. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.

e. Efectuați clic pe **REINSTALEAZĂ** în fereastra afișată

f. Așteptați finalizarea procesului de reinstalare, apoi reporniți sistemul.

Notă
Urmând această procedură de reinstalare, setările personalizate sunt salvate și disponibile în noul produs instalat. Alte setări pot fi comutate înapoi la configurația lor implicită.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru suport, conform descrierii din secțiunea Solicitarea ajutorului (pagina 290).

Nu mai pot utiliza o aplicație

Această problemă apare când încercați să utilizați un program care a funcționat normal înainte de instalarea Bitdefender.

După instalarea Bitdefender ar putea apărea 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 încerci să-l utilizezi.

Acest tip de situație apare când Advanced Threat Defense detectează din greșeală anumite aplicații ca fiind rău intenționate.

Advanced Threat Defense 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 Advanced Threat Defense.

Atunci când se întâmplă aceasta, poți exclude aplicația respectivă de la monitorizarea efectuată de Advanced Threat Defense.

Pentru a adăuga programul în lista de excepții:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **Apărare avansată împotriva amenințărilor** panou, faceți clic **Deschis**.
3. În **Setări** fereastra, faceți clic **Gestionați excepțiile**.
4. Clic **+ Adăugați o excepție**.
5. Introdu calea fișierului executabil pe care vrei să îl excluzi de la scanare în câmpul corespunzător.
   Alternativ, puteți naviga la executabil făcând clic pe butonul de răsfoire din partea dreaptă a interfeței, selectați-l și faceți clic pe **Bine**.
6. Porniți comutatorul de lângă **Apărare avansată împotriva amenințărilor**.
7. Clic **Salvați**.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 290).

Ce trebuie să faci atunci când Bitdefender blochează un site web, un domeniu, o adresă IP sau o aplicație online care este sigură

Bitdefender oferă o experiență de navigare web sigură prin filtrarea întregului trafic web și blocarea oricărui conținut periculos. Cu toate acestea, este posibil ca Bitdefender să considere nesigure un site web, un domeniu, o adresă IP sau o aplicație online care sunt, de fapt, sigure, ceea ce va face ca funcția Bitdefender de scanare a traficului HTTP să le blocheze în mod incorect.

În cazul în care aceleași pagini, domenii, adrese IP sau aplicații online sunt blocate în mod repetat, acestea pot fi adăugate în lista de excepții astfel încât să nu fi scanate de motoarele Bitdefender, asigurând o experiență de navigare pe internet fără probleme.

Pentru a adăuga un site web la **Excepții**:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.

2. În **PREVENIREA AMENINȚĂRILOR ONLINE** panou, faceți clic **Setări**.
3. Clic **Gestionați excepțiile**.
4. Clic **+ Adăugați o excepție**.
5. Introduceți în câmpul corespunzător numele site-ului web, numele domeniului sau adresa IP pe care doriți să o adăugați la excepții.
6. Faceți clic pe comutatorul de lângă **Prevenirea amenințărilor online**.
7. Clic **Salvați** pentru a salva modificările și a închide fereastra.

Numai site-urile, domeniile, adresele IP și aplicațiile în care ai deplină încredere ar trebui adăugate în această listă. Acestea vor fi excluse din procesul de scanare de către motoarele contra amenințărilor, a tentativelor de phishing și fraudelor.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 290).

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. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **FIREWALL** panou, faceți clic **Setări**.
3. În **Reguli** fereastra, faceți clic **Adăugați o regulă**.
4. Se afișează o fereastră nouă unde poți adăuga detalii. Asigură-te că selectezi toate tipurile de rețele disponibile, iar în secțiunea **Permisiune** selectează **Permite**.

Închideți Bitdefender, deschideți aplicația software și încercați din nou să vă conectați la internet.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 290).

Nu pot accesa un dispozitiv din rețeaua mea

În funcție de rețeaua la care ești conectat, firewallul Bitdefender poate bloca conexiunea dintre sistemul tău și un alt dispozitiv (cum ar fi un alt dispozitiv sau o imprimantă). În consecință, nu mai puteți partaja sau imprima fișiere.

În acest caz, cea mai bună soluție este să configurezi Bitdefender să permită în mod automat conexiunile către și de la dispozitivul respectiv, după cum urmează:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **FIREWALL** panou, faceți clic **Setări**.
3. În **Reguli** fereastra, faceți clic **Adăugați o regulă**.
4. Activează opțiunea **Aplică această regulă tuturor aplicațiilor**.
5. Faceți clic pe butonul **Setări avansate**.
6. În caseta **Adresă remote personalizată**, introdu adresa IP a PC-ului sau imprimantei la care dorești să ai acces nerestricționat.

Dacă tot nu vă puteți conecta la dispozitiv, este posibil ca problema să nu fie cauzată de Bitdefender.

Verifică alte cauze posibile, cum ar fi:

- Firewall-ul de pe celălalt dispozitiv poate bloca partajarea fișierelor și imprimantei cu PC-ul tău.
  - Dacă se folosește Windows Firewall, acesta poate fi configurat să permită partajarea de fișiere, după cum urmează:
    - În **Windows 7**:
      1. Fă clic pe **Start**, accesează **Panoul de control** și apoi selectează **System and Security** (Sistem și securitate).
      2. Mergi la **Windows Firewall** și apoi fă clic pe **Allow a program through Windows Firewall** (Permite un program prin Windows Firewall).
      3. Selectați căsuța **File and Printer Sharing**.
    - În **Windows 8** și **Windows 8.1**:
      1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control”

direct în ecranul Start), apoi faceți clic pe pictograma acestuia.

2. Fă clic pe **System and Security**, mergi la {3}Windows Firewall{4} și selectează **Allow an app through Windows Firewall** (Permite o aplicație prin Windows Firewall).
3. Bifează căsuța **File and Printer Sharing** (Partajare fișiere și imprimante) și apoi apasă pe **OK**.

- În **Windows 10** și **Windows 11**:
  1. Introdu "Allow an app through Windows Firewall" în caseta de căutare din bara de sarcini și efectuează clic pe pictogramă.
  2. Fă clic pe **Change settings** (Schimbă setările).
  3. Din lista **Allowed apps and features** (Aplicații și caracteristici permise) bifează caseta **File and Printer Sharing** (Partajare fișiere și imprimantă) și apoi fă clic pe **OK**.

- Dacă se folosește un alt program firewall, consultă documentația sau fișierul de ajutor ale acestuia.

- Cauze generale care pot împiedica folosirea sau conectarea la imprimanta partajată:
  - Poate fi necesar să te conectezi la un cont Windows de administrator pentru a avea acces la imprimanta partajată.
  - Numai anumite dispozitive și anumiți utilizatori pot accesa imprimanta partajată. Dacă partajezi imprimanta ta, verifică restricțiile de acces stabilite pentru aceasta pentru a vedea dacă utilizatorul de pe celălalt dispozitiv o poate accesa. Dacă încerci să te conectezi la o imprimantă partajată, întreabă utilizatorul de pe celălalt dispozitiv dacă îți permite accesul la imprimantă.
  - Imprimanta conectată la dispozitivul tău sau la celălalt nu este partajată.
  - Imprimanta partajată nu este adăugată pe dispozitiv.

> **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 dispoztive 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 au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 290).

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 problemă:

1. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **FIREWALL**, dezactivează butonul pentru a dezactiva această caracteristică.
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 (pagina 290).
   - În cazul în care conexiunea la internet s-a îmbunătățit după dezactivarea firewallului Bitdefender:

a. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.

b. În **FIREWALL** panou, faceți clic **Setări**.

c. Accesează fila **Network Adapters** (Adaptoare rețea) și setează conexiunea la internet ca **Acasă/Birou**.

d. În fila **Settings** (Setări), dezactivează **Port scan protection** (Protecție împotriva scanării porturilor).
În zona **Stealth Mode** (Mod ascuns), fă clic pe **Edit stealth settings** (Editare setări mod ascuns). Activează Modul ascuns pentru adaptorul de rețea la care ești conectat.

e. Închideți Bitdefender, reporniți sistemul ș verificați viteza conexiunii la internet.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 290).

Cum să actualizați Bitdefender în cazul unei conexiuni lente la internet

Dacă dispui de o conexiune lentă la internet (cum ar fi cea de tip dial-up), în timpul procesului de actualizare pot apărea erori.

Pentru a îți păstra sistemul actualizat cu cea mai recentă bază de date cu informațiile privind amenințările a Bitdefender:

1. Clic **Setări** din meniul de navigare de pe Interfața Bitdefender.
2. Selectează **Actualizați** fila.
3. Dezactivează butonul **Actualizare discretă**.
4. Data viitoare când va fi disponibilă o actualizare, ți se va solicita să selectezi actualizarea pe care dorești să o descarci. Selectează doar **Actualizare semnături**.
5. Bitdefender va descărca și instala numai baza de date cu informații privind amenințările.

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 inactivă și se afișează notificarea că serviciile Bitdefender nu răspund.
- Fereastra BitDefender indică faptul că serviciile BitDefender nu răspund.

Problema poate fi cauzată de:

- erori temporare de comunicare între serviciile BitDefender.
- unele dintre serviciile BitDefender sunt oprite.
- alte soluții de securitate rulează pe dispozitivul tău, în același timp cu Bitdefender.

Pentru a remedia această problemă, încearcă următoarele soluții:

1. Așteptați câteva momente pentru a vedea dacă apar schimbări. Eroarea poate fi temporară.
2. Repornește dispozitivul și așteaptă câteva momente până când se încarcă Bitdefender. Deschideți BitDefender pentru a vedea dacă eroarea persistă. De obicei, repornirea dispozitivului rezolvă problema.
3. Verificați dacă aveți instalată orice altă soluție de securitate pentru că ea ar putea perturba funcționarea normală a BitDefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați BitDefender.

   Pentru mai multe informații, consultă capitolul Cum elimin celelalte soluții de securitate? (pagina 120).

Dacă eroarea persistă, vă rugăm să contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea Solicitarea ajutorului (pagina 290).

Filtrul Antispam nu funcționează corespunzător

Acest articol vă ajută să remediați următoarele probleme legate de funcționarea filtrului Antispam 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.**

Mesaje legitime sunt marcate ca [spam]

Mesajele legitime sunt marcate ca [spam] doar pentru că acestea arată ca mesaje spam pentru filtrul antispam Bitdefender. În mod normal, această problemă poate fi rezolvată prin configurarea corespunzătoare a filtrului Antispam.

Bitdefender adaugă automat destinatarii mesajelor tale e-mail într-o Listă de prieteni. Mesajele e-mail primite de la persoanele de contact din Lista de prieteni sunt considerate a fi legitime. Acestea nu sunt verificate de filtrul antispam și, prin urmare, nu sunt niciodată marcate 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.

Dacă folosești unul dintre clienții de e-mail în care se integrează Bitdefender, **indică erorile de detecție**.

> **Notă**
> Bitdefender se integrează în cei mai des utilizați clienți de e-mail printr-o bară de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de e-mail acceptați, consultați Clienți și protocoale de e-mail compatibile (pagina 48).

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 tău de mail, selectează un mesaj e-mail al expeditorului pe care dorești să-l adăugați pe Lista de prieteni.
2. Clic pe butonul **Adăugare 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**.

Vei 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. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În secțiunea **ANTISPAM**, clic pe **Administrare prieteni**.
   Va apărea o fereastră de configurare.
3. Introdu adresa de e-mail de la care dorești să primești mereu mesaje și apoi dă clic pe **ADĂUGARE**. Puteți adăuga oricâte adrese de e-mail doriți.
4. Clic **Bine** pentru a salva modificările și a închide fereastra.

Indică erori 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 de e-mail.
2. Accesați folderul de mesaje nedorite unde sunt mutate mesajele spam.
3. Selectează mesajele legitime pe care Bitdefender le-a marcat incorect ca [spam].
4. Clic pe butonul **Adăugare prieten** din bara de instrumente antispam Bitdefender pentru a adăuga expeditorul pe Lista de prieteni. Pentru confirmare, este posibil să trebuiască să selectezi **OK**. Vei primi întotdeauna mesajele e-mail de la această adresă indiferent ce conțin acestea.
5. Apasă pe **Nu spam** butonul din bara de instrumente antispam Bitdefender (situat în mod normal în partea de sus a ferestrei clientului de e-mail). Mesajul de e-mail va fi mutat în dosarul Inbox.

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.

Încearcă următoarele soluții:

1. Dacă folosești unul dintre clienții de e-mail în care se integrează Bitdefender, **indică mesajele spam nedetectate**.

> **Notă**
> Bitdefender se integrează în cei mai des utilizați clienți de e-mail printr-o bară de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de e-mail acceptați, consultați Clienți și protocoale de e-mail compatibile (pagina 48).

2. **Adăugare spammeri în Lista de spammeri**. Mesajele e-mail primite de la adrese incluse în Lista de spammeri sunt marcate automat ca [spam].

Indică mesajele spam nedetectate

Dacă utilizați un client de e-mail acceptat, puteți indica cu ușurință ce mesaje de e-mail ar fi trebuit detectate ca spam. Acest lucru ajută la îmbunătățirea eficienței filtrului antispam. Urmați acești pași:

1. Deschideți clientul de e-mail.
2. Accesați folderul Inbox.
3. Selectați mesajele spam nedetectate.
4. Faceți clic pe butonul **Este spam** de pe bara de instrumente Bitdefender (localizată în mod normal în partea superioară a ferestrei clientului de e-mail). Mesajele vor fi marcate imediat ca fiind de tip [spam] și mutate în directorul de e-mail-uri nedorite.

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 de e-mail.
2. Accesați folderul de mesaje nedorite unde sunt mutate mesajele spam.
3. Selectați mesajele pe care BitDefender le-a marcat ca [spam].
4. Clic pe butonul **Adăugare 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. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.
2. În **ANTI SPAM** panou, faceți clic **Setări**.
3. Mergeți la fereastra **Gestionare spammeri**.
4. Introduceți adresa de e-mail a spammer-ului și apoi faceți clic pe **Adaugă**. Puteți adăuga oricâte adrese de e-mail doriți.
5. Clic **Bine** pentru a salva modificările și a închide fereastra.

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, clic pe **Protecție** din meniul de navigare al **interfeței Bitdefender**. Accesează secțiunea **Antispam** pentru a verifica dacă această caracteristică este activată.
  Dacă protecția Antispam este dezactivată, aceasta este cauza problemei dvs. Faceți clic pe selectorul corespunzător pentru a activa protecția antispam.
- Protecția Antispam Bitdefender este disponibilă numai pentru clienții de e-mail configurați să primească mesaje e-mail prin protocolul POP3. Aceasta înseamnă următoarele:
  - 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 e-mail prin alt protocol decât POP3 (de exemplu, IMAP4), filtrul Bitdefender Antispam 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 Ultimate Small Business Security 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 (pagina 290).

Nu s-a reușit dezinstalarea Bitdefender

Dacă doriți să ștergeți produsul Bitdefender și observați că procesul este suspendat sau sistemul se blochează, faceți clic pe **Anulare** pentru a abandona acțiunea. Dacă anularea nu este posibilă, reporniți sistemul.

Dacă dezinstalarea eșuează, în sistemul dumneavoastră pot rămâne unele chei de regiștri și fișiere Bitdefender. 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 tău:

- În **Windows 7**:
  1. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
  2. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  3. Clic **ELIMINA** în fereastra care apare.
  4. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
  2. Clic **Dezinstalează un program** sau **Programe si caracteristici**.

3. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
4. Clic **ELIMINA** în fereastra care apare.
5. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

- În **Windows 10** și **Windows 11**:
  1. Clic **start**, apoi faceți clic pe Setări.
  2. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații instalate**.
  3. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  4. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
  5. Clic **ELIMINA** în fereastra care apare.
  6. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

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 acționezi pentru fiecare situație:

- **O soluție Bitdefender a fost instalată anterior și nu ai dezinstalat-o în mod corespunzător.**
  Pentru a remedia această problemă:
  1. Repornește sistemul și accesează-l în Safe Mode. Pentru a afla cum să faci acest lucru, consultă Cum pot să repornesc sistemul în Safe Mode? (pagina 121).
  2. Dezinstalează soluția Bitdefender de pe sistemul tău:

- În **Windows 7**:
  a. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
  b. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  c. Clic **ELIMINA** în fereastra care apare.
  d. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
  e. Repornește sistemul în modul normal.

- În **Windows 8** și **Windows 8.1**:
  a. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
  b. Clic **Dezinstalați un program** sau **Programe si caracteristici**.
  c. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  d. Clic **ELIMINA** în fereastra care apare.
  e. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
  f. Reporniți sistemul în modul normal.

- În **Windows 10** și **Windows 11**:
  a. Clic **start**, apoi faceți clic pe Setări.
  b. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații instalate**.
  c. Găsi **Bitdefender Ultimate Small Business Security** și selectați **Dezinstalează**.
  d. Clic **Dezinstalează** din nou pentru a vă confirma alegerea.
  e. Clic **ELIMINA** în fereastra care apare.

f. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

g. Reporniți sistemul în modul normal.

3. Reinstalează-ți produsul Bitdefender.

- **Ați avut instalată o altă soluție de securitate înainte, iar aceasta nu a fost dezinstalată corespunzător.**
  Pentru a rezolva asta:

  1. Reporniți sistemul și intrați în modul Safe. Pentru a afla cum să faceți acest lucru, consultați Cum pot să repornesc sistemul în Safe Mode? (pagina 121).
  2. Șterge cealaltă soluție de securitate din sistem:
     - În **Windows 7**:
       a. Clic **start**, mergi la **Panou de control** și faceți dublu clic **Programe si caracteristici**.
       b. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Ștergere**.
       c. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
     - În **Windows 8** și **Windows 8.1**:
       a. Din ecranul de pornire Windows, localizați **Panou de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul Start), apoi faceți clic pe pictograma acestuia.
       b. Clic **Dezinstalează un program** sau **Programe si caracteristici**.
       c. Găsiți numele programului pe care doriți să îl eliminați și selectați **Elimina**.
       d. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.
     - În **Windows 10** și **Windows 11**:
       a. Clic **start**, apoi faceți clic pe Setări.

b. Apasă pe **Sistem** pictograma din zona Setări, apoi selectați **Aplicații instalate**.

c. Găsiți numele programului pe care doriți să îl eliminați și selectați **Dezinstalează**.

d. Așteptați finalizarea procesului de dezinstalare, apoi reporniți sistemul.

Pentru a dezinstala celălalt software în mod corect, mergi pe site-ul web al producătorului și lansează instrumentul de dezinstalare sau contactează direct producătorul, solicitând instrucțiunile de dezinstalare.

3. Reporniți sistemul în modul normal și reinstalați Bitdefender.

Situația nu s-a rezolvat deși ați urmat toți pașii de mai sus.

Pentru a rezolva asta:

1. Reporniți sistemul și intrați în modul Safe. Pentru a afla cum să faceți acest lucru, consultați Cum pot să repornesc sistemul în Safe Mode? (pagina 121).
2. Cu ajutorul funcției System Restore din Windows poți restabili dispozitivul la o dată anterioară instalării produsului Bitdefender.
3. Reporniți sistemul în modul normal și contactați reprezentanții serviciului de asistență, după cum este specificat în secțiunea Solicitarea ajutorului (pagina 290).

3.5.2. Eliminarea amenințărilor din sistemul tău

Amenințările vă pot afecta sistemul în moduri diferite, iar modul de acțiune al Bitdefender depinde de tipul de atac al amenințării. Deoarece amenințările 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 amenințarea din sistemul dumneavoastră. În astfel de cazuri, este necesară intervenția dumneavoastră.

- Mediu de salvare (pagina 144)
- Ce poți face când Bitdefender găsește amenințări pe dispozitivul tău? (pagina 145)

- Cum elimin o amenințare dintr-o arhivă? (pagina 146)
- Cum elimin o amenințare dintr-o arhivă de e-mail? (pagina 147)
- Ce trebuie să fac dacă suspectez că un fișier este periculos? (pagina 148)
- Ce reprezintă fișierele protejate prin parolă din jurnalul de scanare? (pagina 149)
- Ce reprezintă elementele omise din jurnalul de scanare? (pagina 149)
- Ce reprezintă fișierele supracomprimate din jurnalul de scanare? (pagina 149)
- De ce Bitdefender a șters în mod automat un fișier infectat? (pagina 150)

Dacă nu puteți găsi problema dvs. aici sau dacă soluțiile prezentate nu o rezolvă, puteți contacta reprezentanții de asistență tehnică Bitdefender, așa cum este prezentat în capitolul Solicitarea ajutorului (pagina 290).

Mediu de salvare

Mediu de recuperare este o caracteristică a Bitdefender care îți permite să scanezi și să dezinfectezi toate partițiile unității hard din/ de pe sistemul de operare.

Mediul de recuperare Bitdefender este integrat cu Windows RE.

Pornirea sistemului în Modul de recuperare

Poți intra în Modul de recuperare numai din produsul tău Bitdefender, după cum urmează:

1. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
2. În **ANTIVIRUS** panou, faceți clic **Deschis**.
3. Selectează **Deschide** din dreptul opțiunii **Mediu de recuperare**.
4. Selectează **REPORNIRE** în fereastra care se deschide.
   Mediul de recuperare Bitdefender se încarcă în câteva momente.

Scanarea sistemului în Modul de recuperare

Pentru scanarea sistemului în Modul de recuperare:

1. Accesează Mediul de recuperare, conform descrierii din Pornirea sistemului în Modul de recuperare (pagina 144).
2. Procesul de scanare Bitdefender începe automat imediat ce sistemul este încărcat în Mediul de recuperare.
3. Așteptați finalizarea procesului de scanare. Dacă este detectată o amenințare, urmează instrucțiunile pentru îndepărtarea acesteia.
4. Pentru a ieși din Mediul de recuperare, efectuează clic pe butonul Închidere din fereastra cu rezultatele scanării.

Ce poți face când Bitdefender găsește amenințări pe dispozitivul tău?

Este posibil să afli că există amenințări pe dispozitivul tău într-unul din următoarele moduri:

- Ți-ai scanat dispozitivul și Bitdefender a găsit elemente infectate pe acesta.
- O alertă de amenințări te informează că Bitdefender a blocat una sau mai multe amenințări pe dispozitivul tău.

În astfel de situații, actualizează Bitdefender pentru a te asigura că ai cele mai recente baze de date cu informații privind amenințările și efectuează o scanare a sistemului pentru analizarea acestuia.

După finalizarea scanării sistemului, selectează acțiunea dorită pentru elementele infectate (dezinfectare, ștergere, mutare în carantină).

Avertizare
În cazul în care consideri că fișierul face parte din sistemul de operare Windows sau că nu este un fișier infectat, nu urma acești pași și contactează 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 ștergi fișierul/fișierele manual:

Prima metodă poate fi utilizată în modul normal:

1. Dezactivați protecția antivirus în timp real Bitdefender:
   a. Clic **Protecție** pe meniul de navigare de pe Interfața Bitdefender.

b. În **ANTIVIRUS** panou, faceți clic **Deschis**.

c. În **Avansat** fereastra, stinge **Bitdefender Shield**.

2. Afișează obiecte ascunse în Windows. Pentru a afla cum să faceți acest lucru, consultați Cum pot afișa elementele ascunse din Windows? (pagina 119).
3. Mergi la locația unde se găsește fișierul infectat (verifică jurnalul de scanare) și șterge-l.
4. Activați protecția antivirus în timp real Bitdefender.

În cazul în care prima metodă nu a reușit să elimine infecția:

1. Reporniți sistemul și intrați în modul Safe. Pentru a afla cum să faceți acest lucru, consultați Cum pot să repornesc sistemul în Safe Mode? (pagina 121).
2. Afișează obiecte ascunse în Windows. Pentru a afla cum să faceți acest lucru, consultați Cum pot afișa elementele ascunse din Windows? (pagina 119).
3. Navigați la locația fișierului infectat (verificați jurnalul de scanare) și ștergeți-l.
4. Repornește sistemul în mod normal.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 290).

Cum elimin o amenințare 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 amenințărilor din acestea însă nu poate lua niciun fel de măsură în acest sens.

Dacă Bitdefender anunță că a fost detectată o amenințare într-o arhivă și nu este disponibilă nicio acțiune, aceasta înseamnă că eliminarea

amenințării nu este posibilă din cauza restricțiilor legate de setările referitoare la permisiunile arhivelor.

Iată cum poți elimina o amenințare stocată într-o arhivă:

1. Identifică arhiva care conține amenințarea în urma unei scanări a sistemului.
2. Dezactivați protecția antivirus în timp real Bitdefender:
   a. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
   b. În **ANTIVIRUS** panou, faceți clic **Deschis**.
   c. În **Avansat** fereastra, stinge **Bitdefender Shield**.
3. Accesează locația arhivei și dezarhiveaz-o utilizând o aplicație de arhivare, cum ar fi WinZip.
4. Identifica fișierul infectat și șterge-l.
5. Șterge arhiva inițială pentru a te asigura că fișierul infectat este eliminat în totalitate.
6. Recomprimă 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 a sistemului pentru a vă asigura că sistemul nu este infectat.

> **Notă**
> Este important de reținut faptul că o amenințare aflată într-o arhivă nu reprezintă o amenințare imediată la adresa sistemului tău deoarece trebuie să fie dezarhivată și executată pentru a putea infecta calculatorul.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 290).

Cum elimin o amenințare dintr-o arhivă de e-mail?

Bitdefender poate de asemenea să identifice amenințări 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 poți elimina o amenințare stocată într-o arhivă de e-mail:

1. Scanează baza de date de e-mailuri cu Bitdefender.
2. Dezactivați protecția antivirus în timp real Bitdefender:
   a. Clic **Protecție** din meniul de navigare de pe Interfața Bitdefender.
   b. În **ANTIVIRUS** panou, faceți clic **Deschis**.
   c. În **Avansat** fereastra, stinge **Bitdefender Shield**.
3. Deschide raportul de scanare și utilizeaza 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. Arhivează directorul în care se află mesajul infectat.
   - În Microsoft Outlook 2007: Din meniul File (Fișier), selectează Data File Management (Administrare fișiere de date). Alege fișierele (.pst) pe care intenționezi să le compactezi, apoi selectează Settings (Setări). Clic pe Compact Now (Compactează acum).
   - În Microsoft Outlook 2010/2013/2016: Din meniul File (Fișier), selectează Info (Informații), apoi Account settings (Add and remove accounts or change existing connection settings) [Setări cont (Adăugare și eliminare conturi sau modificare setări de conectare existente)]. Apoi selectează Data File (Fișier de date), fișierele (.pst) pe care intenționezi să le compactezi și alege opțiunea Settings (Setări). Clic pe Compact Now (Compactează acum).
6. Activați protecția antivirus în timp real Bitdefender.

Dacă aceste informații nu au fost utile, puteți contacta Bitdefender pentru asistență, așa cum este descris în secțiunea Solicitarea ajutorului (pagina 290).

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 te asigura că sistemul tău este protejat:

1. Execută o **Scanare de sistem** cu Bitdefender. Pentru a afla cum să faci acest lucru, consultă How do I scan my system?.
2. Dacă procesul de scanare nu a detectat nimic, dar încă ai dubii cu privire la fișier, contactează reprezentanții serviciul de asistență pentru ajutor.
   Pentru a afla cum să faci acest lucru, consultă Solicitarea ajutorului (pagina 290).

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-ti proteja dispozitivul. Dacă doriți să scanați acele fișiere folosind Bitdefender, trebuie să contactați producătorul produsului pentru a obține mai multe detalii despre respectivele fișiere.

Noi îți recomandăm să ignori acele fișiere deoarece acestea nu reprezintă o amenințare pentru sistemul tău.

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.

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.

Supracomprimarea 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 în timp real, la accesare, dacă este cazul.

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 amenințări, dezinfecția nu este posibilă deoarece fișierul detectat este complet rău intenționat. În astfel de cazuri, fișierul infectat este șters de pe disc.

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.

4. ANTIVIRUS PENTRU MAC

4.1. Ce este Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac este un scanner antivirus puternic, care poate detecta și elimina toate tipurile de programe periculoase ("amenințări"), incluzând:

- ransomware
- adware
- viruși
- spyware
- Troieni
- keylogger
- viermi

Această aplicație detectează și elimină nu numai amenințările pentru Mac, ci și amenințările pentru Windows, împiedicându-te astfel să transmiți fișiere infectate familiei, prietenilor și colegilor care utilizează calculatoare.

4.2. Instalare și dezinstalare

Acest capitol acoperă următoarele subiecte:

- Cerințe de sistem (pagina 151)
- Instalarea Bitdefender Antivirus for Mac (pagina 152)
- Dezinstalarea Bitdefender Antivirus for Mac (pagina 156)

4.2.1. Cerințe de sistem

Poți instala Bitdefender Antivirus for Mac pe computerele Macintosh cu sistem de operare OS X Yosemite (10.10) sau o versiune mai nouă.

Mac-ul tău trebuie să aibă minimum 1 GB de spațiu disponibil pe hard disk.

Este necesar să fiți conectați la internet pentru a înregistra și actualiza Bitdefender Antivirus for Mac.

Notă

Bitdefender Anti-tracker și Bitdefender VPN pot fi instalate doar pe sistemele de operare macOS 10.12 sau versiuni mai noi.

Cum să afli versiunea de macOS și informații hardware despre Mac-ul tău

Efectuează clic pe pictograma Apple din colțul din stânga sus al ecranului și selectează Despre **acest Mac**. În fereastra care apare, vei vedea detalii despre versiunea sistemului tău de operare, precum și alte informații utile. Efectuează clic pe **Raport sistem** pentru a vedea informații detaliate despre componentele hardware.

4.2.2. Instalarea Bitdefender Antivirus for Mac

Aplicația Bitdefender Antivirus for Mac poate fi instalată prin accesarea contului tău Bitdefender astfel:

1. Conectează-te ca administrator.
2. Accesează: https://central.bitdefender.com.
3. Conectează-te la contul Bitdefender folosind adresa ta de e-mail și parola.
4. Accesează secțiunea **Dispozitivele mele** și apoi apasă pe **INSTALEAZĂ PROTECȚIA**.
5. Alege una dintre cele două opțiuni disponibile:
   - **Protejează acest dispozitiv**
     a. Selectează această opțiune și apoi deținătorul dispozitivului. Dacă dispozitivul aparține altcuiva, selectează opțiunea corespunzătoare.
     b. Salvează fișierul de instalare.
   - **Protejează alte dispozitive**
     a. Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
     b. Efectuează clic pe **TRIMITE LINK DE DESCĂRCARE**.
     c. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**.

Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.

d. Pe dispozitivul pe care dorești să instalezi produsul Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

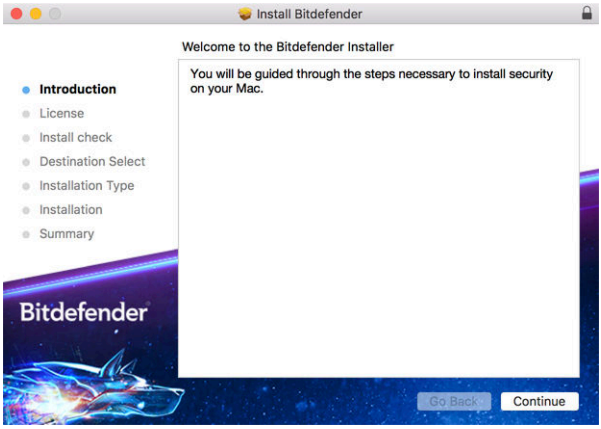
6. Rulați produsul Bitdefender descărcat.
7. Urmează pașii de instalare.

Proces de instalare

Pentru a instala Bitdefender Antivirus for Mac:

1. Faceți clic pe fișierul descărcat. Veți lansa astfel programul de instalare, care vă va ghida pe parcursul procesului de instalare.
2. Urmează indicațiile programului asistent de instalare.

Pasul 1 - Fereastra de întâmpinare



Efectuează clic pe **Continuare**.

Pasul 2 - Citește Contractul de abonament

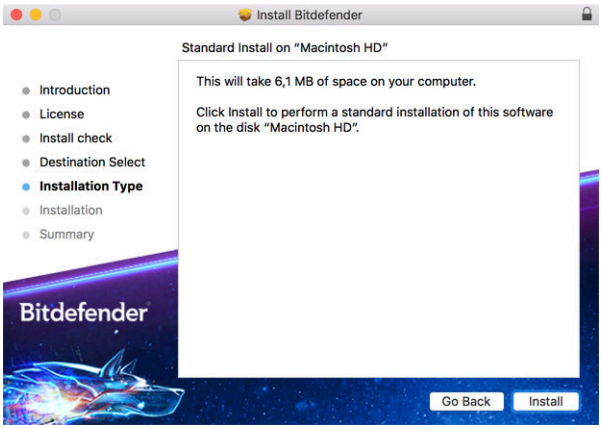
Înainte de a contninua instalarea, este necesar să îți exprimi acordul cu privire la clauzele Contractului de abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Antivirus for Mac.

Din această fereastră poți selecta și limba în care dorești să instalezi produsul.

Efectuează clic pe **Continuare**, apoi pe **De acord**.

> **Important**
> Dacă nu ești de acord cu acești termeni, efectuează clic pe **Continuare** și apoi pe **Nu sunt de acord** pentru a anula procesul de instalare.

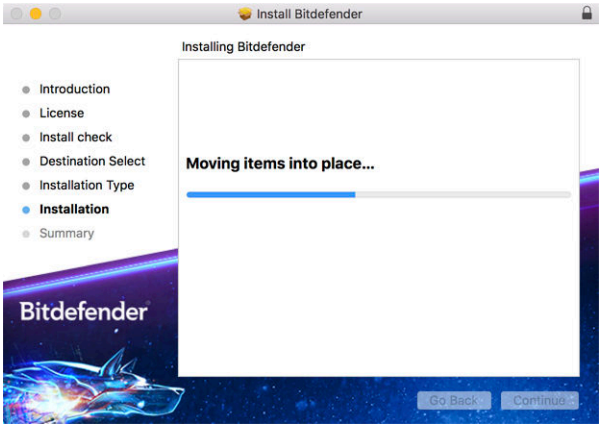
Pasul 3 - Inițiază instalarea



Bitdefender Antivirus for Mac va fi instalat în Macintosh HD/Library/Bitdefender. Calea de instalare nu poate fi modificată.

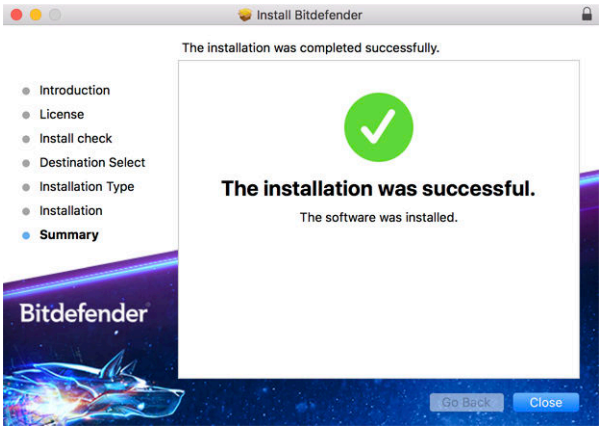
Faceți clic pe **Instalează** pentru a inițiа instalarea.

Pasul 4 - Instalarea Bitdefender Antivirus for Mac



Așteptați până când instalarea este finalizată și apoi faceți clic pe **Continuă**.

Pasul 5 - Finalizare



Faceți clic pe **Închide** pentru a închide fereastra programului de instalare.

Procesul de instalare s-a încheiat.

Important

- Dacă instalezi Bitdefender Antivirus for Mac pe un sistem de operare macOS High Sierra 10.13.0 sau o versiune mai nouă, va apărea notificarea **Extensie sistem blocată**. Această notificare te informează că extensiile semnate de Bitdefender au fost blocate și trebuie activate manual. Apasă pe OK pentru a continua. În fereastra Bitdefender Antivirus for Mac care apare, apasă pe linkul **Securitate și Confidențialitate**. Apasă pe **Permite** din partea de jos a ferestrei sau selectează Bitdefender SRL din listă și apoi apasă pe **OK**.
- Dacă instalezi Bitdefender Antivirus for Mac pe sistemul de operare macOS Mojave 10.14 sau o versiune mai nouă, se afișează o fereastră nouă care te informează că trebuie să **Permiți accesul Bitdefender la întregul disc** și să **Permiți încărcarea Bitdefender**. Urmează instrucțiunile de pe ecran pentru a configura corespunzător produsul.

4.2.3. Dezinstalarea Bitdefender Antivirus for Mac

Deoarece este o aplicație complexă, Bitdefender Antivirus for Mac nu poate fi dezinstalat în modul obișnuit, prin transferarea pictogramei aplicației din directorul **Aplicații** în directorul Trash.

Pentru a dezinstala Bitdefender Antivirus for Mac, urmează acești pași:

1. Deschide o fereastră **Finder**, apoi accesează directorul **Aplicații**.
2. Deschide directorul Bitdefender în **Aplicații** apoi efectuează dublu clic pe **BitdenderUninstaller**.
3. Selectează opțiunea de dezinstalare preferată.

   Notă
   Dacă încerci să dezinstalezi doar aplicația Bitdefender VPN, selectează **Dezinstalare VPN**.

4. Fă clic pe **Dezinstalare** și așteaptă finalizarea procesului.
5. Apasă pe **Închidere** pentru a finaliza.

   Important
   În cazul apariției unei erori, puteți contacta serviciul de asistență clienți al Bitdefender, așa cum se descrie în Solicitarea ajutorului (pagina 290).

4.3. Introducere

Acest capitol include următoarele subiecte:

- Deschiderea Bitdefender Antivirus for Mac (pagina 157)
- Fereastră principală aplicație (pagina 158)
- Pictogramă aplicație în Dock (pagina 159)
- Meniu de navigare (pagina 160)
- Mod întunecat (pagina 160)

4.3.1. Deschiderea Bitdefender Antivirus for Mac

Aveți mai multe modalități prin care puteți deschide Bitdefender Antivirus for Mac.

- Efectuează clic pe pictograma Bitdefender Antivirus for Mac din bara de lansare.
- Apasă pe pictograma din bara de meniu și alege **Deschide interfața Antivirus**.

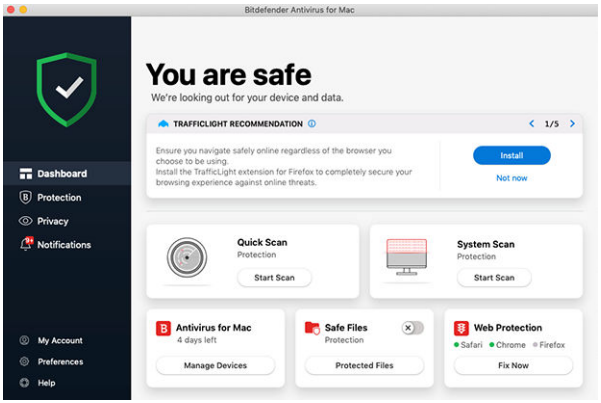
- Deschide o fereastră Finder, accesează Aplicații și efectuează dublu clic pe pictograma **Bitdefender Antivirus for Mac**.

  Important
  Prima dată când deschizi Bitdefender Antivirus for Mac pe macOS Mojave 10.14 sau o versiune mai nouă, se va afișa o recomandare de protecție. Această recomandare apare deoarece avem nevoie de anumite drepturi de acces pentru a scana întregul sistem în vederea identificării amenințărilor. Pentru a ne acorda aceste drepturi, este necesar să fii autentificat ca administrator și să parcurgi pașii următori:

  1. Accesează linkul **Preferințe sistem**.
  2. Apasă pe pictograma și apoi tastează datele tale de autentificare ca administrator.
  3. Se va deschide o nouă fereastră. Trage fișierul **BDLDaemon** în lista aplicațiilor permise.

4.3.2. Fereastră principală aplicație

Bitdefender Antivirus for Mac 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 parcurge interfața Bitdefender, în partea din stânga sus este afișat un asistent de introducere care conține detalii despre cum să interacționezi cu produsul și cum să îl configurezi. Selectează săgeata

dreapta pentru a continua să primești indicații sau **Renunță la tur** pentru a închide asistentul.

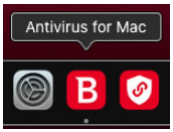
Bara de stare din partea de sus a ferestrei te informează cu privire la starea de securitate a sistemului tău folosind mesaje explicite și culori sugestive. Dacă Bitdefender Antivirus for Mac nu prezintă avertismente, bara de stare este verde. Atunci când a fost detectată o problemă de securitate, culoarea barei de stare devine roșie. Pentru a vedea informații detaliate despre erori și cum să le remediezi, consultă Remedierea problemelor (pagina 173).

Pentru a-ți oferi o funcționare eficientă și o protecție sporită în timp ce desfășori diferite activități, **Bitdefender Autopilot** va acționa ca asistentul tău personal în materie de securitate. În funcție de activitatea pe care o desfășori, fie că e vorba de activități profesionale sau de efectuarea de plăți online, Bitdefender Autopilot îți va oferi recomandări contextuale în funcție de modul de utilizare a dispozitivului tău și nevoile tale. Acest lucru te va ajuta să descoperi și să beneficiezi de avantajele aduse de caracteristicile incluse în aplicația Bitdefender Antivirus for Mac.

Din meniul de navigare din partea stângă, poți accesa secțiunile Bitdefender pentru a vedea detalii despre configurație și setări administrative avansate (filele **Protecție** și **Confidențialitate**), notificări, contul tău **Bitdefender** și secțiunea de **Preferințe**. De asemenea, ne poți contacta (fila **Asistență**) dacă ai nevoie de răspunsuri la întrebări sau în cazul în care apare ceva neașteptat.

4.3.3. Pictogramă aplicație în Dock

Pictograma Bitdefender Antivirus for Mac este vizibilă în Dock imediat ce deschizi aplicația. Pictograma din Dock îți oferă o metodă simplă de scanare a fișierelor și directoarelor pentru a identifica amenințările. Trebuie doar să aduci fișierul sau directorul respectiv peste pictograma Dock folosind drag & drop și scanarea va porni imediat.



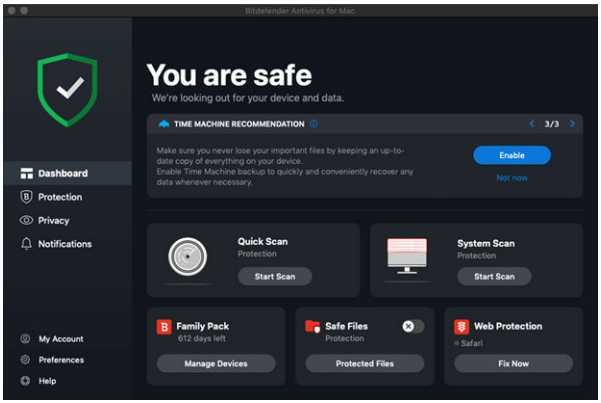
4.3.4. Meniu de navigare

În partea stângă a interfeței Bitdefender se regăsește meniul de navigare, care îți permite să accesezi rapid caracteristicile Bitdefender de care ai nevoie pentru gestionarea produsului tău. Filele disponibile în această secțiune sunt următoarele:

- **Panoul de control**. De aici, poți rezolva rapid problemele de securitate, poți vizualiza recomandări în funcție de nevoile și tiparele de utilizare ale sistemului tău, poți efectua acțiuni rapide și accesa contul tău Bitdefender pentru a gestiona dispozitivele pe care le-ai adăugat la abonamentul tău Bitdefender.
- **Protecție**. De aici, poți lansa sarcini de scanare antivirus, poți adăuga fișiere în lista de excepții, poți proteja fișiere și aplicații împotriva atacurilor de tip ransomware, îți poți securiza backup-urile Time Machine și îți poți configura protecția în timp ce navighezi pe Internet.
- **Confidențialitate**. De aici, poți deschide aplicația Bitdefender VPN și poți instala extensia Anti-tracker în browserul tău web.
- **Notificări**. De aici, poți vedea detalii despre acțiunile întreprinse asupra fișierelor scanate.
- **Contul meu**. De aici, poți vizualiza detaliile contului tău Bitdefender și ale abonamentului care îți protejează dispozitivul și poți comuta între conturi dacă este cazul.
- **Preferințe**. De aici, poți configura setările Bitdefender.
- **Ajutor**. De aici, ori de câte ori ai nevoie de asistență pentru a rezolva o situație în legătură cu produsul Bitdefender, poți contacta departamentul de Asistență tehnică. De asemenea, ne poți trimite feedback pentru a ne ajuta să îmbunătățim produsul.

4.3.5. Mod întunecat

Pentru a-ți feri ochii de lumina puternică atunci când lucrezi noaptea sau într-un mediu fără lumină, Bitdefender Antivirus for Mac acceptă Modul întunecat pentru Mojave 10.14 sau mai recent. Culorile interfeței au fost optimizate astfel încât să poți utiliza Mac-ul fără a-ți obosi ochii. Interfața Bitdefender Antivirus for Mac se ajustează singură în funcție de setările de aspect ale dispozitivului tău.



4.4. Protecția împotriva softurilor periculoase

Acest capitol include următoarele subiecte:

4.4.1. Recomandări de utilizare

Pentru a îți proteja sistemul împotriva amenințărilor și pentru a preveni infectarea accidentală a altor sisteme, respectă aceste bune practici:

- Ține **Bitdefender Shield** activat pentru a permite scanarea automată a fișierelor sistemului de Bitdefender Antivirus for Mac.
- Actualizează-ți produsul Bitdefender Antivirus for Mac pentru a avea acces la cele mai recente informații despre amenințări și actualizări de produse.
- Verificați și soluționați în mod regulat problemele raportate de Bitdefender Antivirus for Mac. Pentru informații detaliate, consultați capitolul Remedierea problemelor (pagina 173).
- Verifică jurnalul detaliat de evenimente privind activitatea Bitdefender Antivirus for Mac pe computerul tău. De fiecare dată când are loc un eveniment relevant pentru securitatea sistemului sau a datelor tale, se adaugă un nou mesaj în secțiunea de Notificări Bitdefender. Pentru mai multe informații, accesează Notificări (pagina 174).
- Vă sugerăm să urmați aceste recomandări de utilizare:
  - Obișnuiți-vă să scanați fișierele pe care le descărcați de pe o memorie externă de stocare (precum un stick USB sau un CD), în special atunci când sursa nu vă este cunoscută.
  - În cazul unui fișier DMG, instalați-l și apoi scanați conținutul acestuia (fișierele din volumul/imaginea instalată).

  Cel mai ușor mod de a scana un fișier, un director sau un volum este prin folosirea drag & drop pentru a-l poziționa deasupra ferestrei Bitdefender Antivirus for Mac sau pictogramei Dock.

Nu este necesară nicio altă configurație sau acțiune. Cu toate acestea, dacă doriți, vă puteți ajusta setările și preferințele pentru a corespunde mai bine necesităților dvs. Pentru mai multe informații, consultă capitolul Configurarea preferințelor (pagina 177).

4.4.2. Scanarea Mac-ului dumneavoastră

În afara caracteristicii **Bitdefender Shield**, care monitorizează cu regularitate aplicațiile instalate în vederea identificării acțiunilor de tipul amenințărilor și împiedicării pătrunderii noilor amenințări în sistemul tău, îți poți scana Mac-ul sau anumite fișiere oricând dorești.

Cel mai ușor mod de a scana un fișier, un director sau un volum este prin folosirea drag & drop pentru a-l poziționa deasupra ferestrei Bitdefender Antivirus for Mac sau pictogramei Dock. Va apărea programul asistent de scanare, care te va ghida în procesul de scanare.

Puteți începe o operațiune de scanare și astfel:

1. Selectează **Protecție** din meniul de navigare al interfeței Bitdefender.
2. Selectează fila **Antivirus**.
3. Efectuează clic pe unul dintre cele trei butoane de scanare pentru a iniția scanarea dorită.
   - **Quick Scan (Scanare rapidă)** - verifică dacă există amenințări în cele mai vulnerabile locații din sistemul tău (de exemplu, directoarele care conțin documentele, fișierele descărcate de pe internet sau din e-mail și fișierele temporare ale fiecărui utilizator).
   - **Scanare sistem** - efectuează o verificare completă pentru a identifica amenințările din întregul sistem. Toate dispozitivele conectate vor fi, de asemenea, scanate.

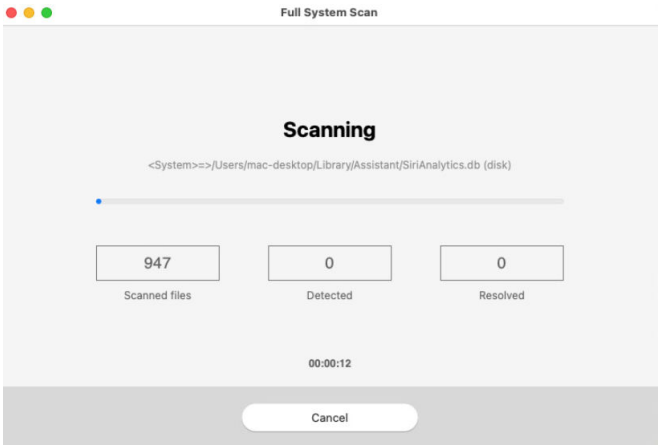
     Notă
     În funcție de dimensiunea hard disk-ului dumneavoastră, scanarea întregului sistem poate dura până la o oră sau chiar mai mult. Pentru o mai bună performanță, se recomandă să nu rulați această operațiune în timp ce efectuați alte operațiuni care folosesc intensiv resursele (cum ar fi editarea video).

     În funcție de preferințele tale, poți alege să nu scanezi anumite volume instalate prin adăugarea acestora în lista de **Excepții** din fereastra Protecție.
   - **Custom Scan (Scanare personalizată)** - te ajută să verifici anumite fișiere, foldere sau volume pentru a identifica amenințările.

De asemenea, poți porni o Scanare de sistem sau o Scanare rapidă din Panoul de control.

4.4.3. Asistent scanare

Atunci când inițiezi o scanare, va apărea expertul de scanare Bitdefender Antivirus for Mac.



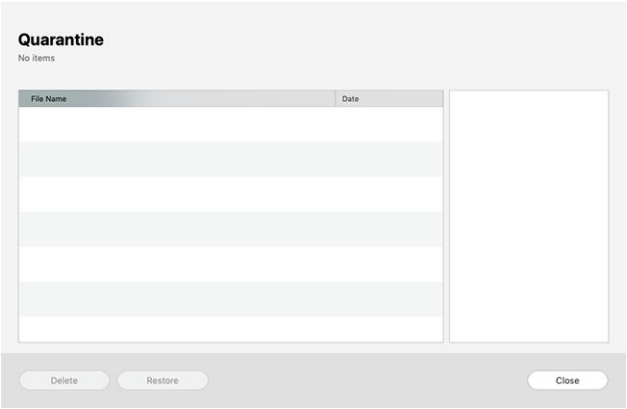
În timpul fiecărei scanări sunt afișate informații în timp real despre amenințările detectate și soluționate.

Așteaptă ca Bitdefender Antivirus for Mac să finalizeze scanarea.

> **Notă**
> Procesul de scanare poate dura cateva minute, în funcție de complexitatea scanării.

4.4.4. Carantină

Bitdefender Antivirus for Mac permite izolarea fișierelor infectate sau suspecte într-o zonă sigură, numită carantină. Atunci când sunt în carantină, amenințările sunt inofensive, pentru că nu pot fi executate sau citite.



Secțiunea Carantină afișează toate fișierele izolate în directorul Carantină.

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

Pentru a vizualiza lista tuturor obiectelor adăugate în carantină:

1. Clic **Protecție** în meniul de navigare din interfața Bitdefender.
2. Apasă pe **Deschide** în panoul **Carantină**.

4.4.5. Bitdefender Shield (protecție în timp real)

Bitdefender oferă protecție în timp real împotriva unei game largi de amenințări prin scanarea tuturor aplicațiilor instalate, a versiunilor actualizate a acestora, precum și a fișierelor noi și modificate.

Pentru dezactivarea protecției în timp real:

1. Selectează **Preferințe** din meniul de navigare al interfeței Bitdefender.
2. Dezactivează **Bitdefender Shield** din fereastra **Protecție**.

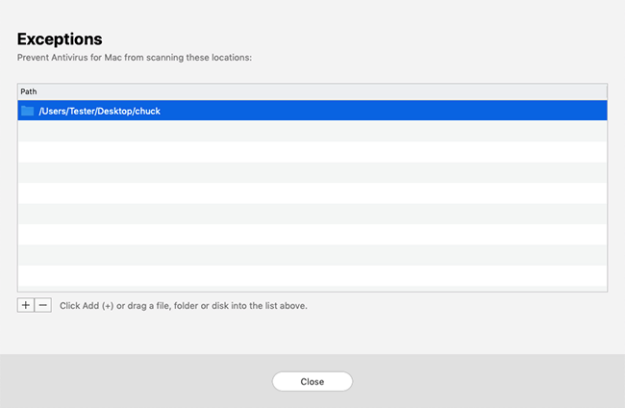
Avertizare

Aceasta este o problemă majoră de securitate. Îți recomandăm să dezactivezi protecția în timp real pentru cât mai puțin timp posibil. Dacă protecția în timp real este dezactivată, nu vei mai fi protejat împotriva amenințărilor.

4.4.6. Excepții scanare

Puteți configura Bitdefender Antivirus for Mac astfel încât să nu scaneze anumite fișiere, dosare sau informațiile de pe o întreagă partiție. De exemplu, ați putea exclude de la scanare:

- Fișiere identificate eronat ca infectate (cunoscute drept "fals pozitive")
- Fișierele care duc la erori de scanare
- Volume de backup



Lista de excepții conține căile de acces către fișierele ce au fost excluse de la scanare.

Pentru a accesa lista de excepții:

1. Clic **Protecție** în meniul de navigare din interfața Bitdefender.
2. Apasă pe **Deschide** în panoul **Excepții**.

Există două modalități prin care poți crea o excepție de la scanare:

- Folosește metoda drag & drop și trage un fișier, director sau volum deasupra listei de excepții.
- Apasă pe butonul marcat cu semnul plus (+), situat sub lista excepțiilor. Apoi alege fișierul, directorul sau volumul care urmează a fi exclus din operațiunea de scanare.

Pentru a șterge o excepție de la scanare, selecteaz-o din listă și apasă pe butonul marcat cu semnul minus (-), situat sub lista excepțiilor.

4.4.7. Protecție web

Bitdefender Antivirus for Mac folosește extensii TrafficLight pentru o protecție completă a experienței tale de navigare pe internet. Extensiile TrafficLight interceptează, procesează și filtrează întregul trafic internet, blocând conținutul periculos.

Extensiile sunt compatibile și se integrează cu următoarele browsere web: Mozilla Firefox, Google Chrome și Safari.

Activarea extensiilor TrafficLight

Pentru a activa extensiile TrafficLight:

1. Selectează **Remediază acum** din secțiunea **Protecție web** a Panoului de control.
2. Se deschide fereastra **Protecție web**.
   Se va afișa browser-ul web instalat pe sistemul tău. Pentru a instala extensia TrafficLight în browserul tău, selectează **Obținere extensie**.
3. Se face redirecționarea către:
   https://bitdefender.com/solutions/trafficlight.html
4. Selectează **Descărcare gratuită**.
5. Urmați pașii pentru instalarea extensiei TrafficLight corespunzătoare browser-ului dumneavoastră web.

Administrarea setărilor extensiilor

Sunt disponibile mai multe funcții pentru protecția dumneavoastră împotriva tuturor tipurilor de amenințări pe care le puteți întâlni în timpul browsing-ului web. Pentru a le accesa, apasă pictograma în formă de semafor de lângă setările browser-ului tău și apoi apasă butonul ⚙ **Setări**:

- **Setări Bitdefender TrafficLight**
  - Protecție web - împiedică accesarea site-urilor web utilizate pentru malware, phishing și atacuri frauduloase.
  - Asistență la căutare - oferă avertizări în avans cu privire la site-urile web riscante din rezultatele căutării tale.
- **Excepții**
  Dacă te afli pe site-ul web pe care dorești să-l adaugi la excepții, selectează opțiunea **Adaugă în listă acest site web**.

Dacă dorești să adaugi un alt site web, introdu adresa acestuia în câmpul corespunzător și apoi selectează ⊕.
Nu se vor afișa avertizări dacă paginile excluse includ amenințări. Acesta este motivul pentru care această listă trebuie cuprindă doar site-urile web în care aveți încredere deplină.

Rating-ul de pagină și alerte

În funcție de cum TrafficLight clasifică pagina web pe care o vizualizezi la momentul respectiv, una sau mai multe dintre următoarele pictograme sunt afișate în zona corespunzătoare:

Aceasta este o pagină sigură. Îți poți continua activitatea.

Această pagină poate avea conținut periculos. Procedează cu precauție dacă decizi să o vizitezi.

Ar trebui să părăsești această pagină web acum întrucât conține malware sau alte amenințări.

În Safari, pictogramele TrafficLight sunt pe fundal negru.

4.4.8. Anti-tracker

Multe dintre site-urile web pe care le accesezi utilizează instrumente de urmărire de tip tracker pentru a colecta informații despre comportamentul tău, fie pentru a le distribui unor companii terțe, fie pentru a afișa anunțuri mai relevante pentru tine. Astfel, proprietarii site-urilor web fac bani pentru a putea oferi conținut gratuit sau pentru a continua să funcționeze. Pe lângă colectarea de informații, tracker-ele pot încetini experiența ta de navigare sau îți pot afecta lățimea de bandă.

Când extensia Bitdefender Anti-tracker este activată în browserul web, aceasta te ajută să eviți să fii monitorizat, astfel încât datele tale rămân confidențiale în timp ce navighezi online, precum și să reduci timpul necesar pentru încărcarea site-urilor web.

Extensia Bitdefender este compatibilă cu următoarele browsere web:

- Google Chrome
- Mozilla Firefox
- Safari

Tracker-ele pe care le detectăm sunt grupate în următoarele categorii:

- **Publicitate** - se utilizează pentru a analiza traficul de pe site-urile web, comportamentul utilizatorilor sau tiparele de trafic generat de utilizatori.
- **Interacțiunea cu clienții** - se utilizează pentru a măsura interacțiunea utilizatorilor cu diferite forme de introducere de informații, cum ar fi chat sau suport.
- **Esențiale** - se utilizează pentru a monitoriza funcționalitățile de importanță critică ale paginilor web.
- **Date de analiză site** - se utilizează pentru a colecta date referitoare la utilizarea paginilor web.
- **Rețele de socializare** - se utilizează pentru a monitoriza audiența pe rețelele de socializare, activitatea și implicarea utilizatorilor pentru diferite platforme de socializare.

Activarea Bitdefender Anti-tracker

Pentru a activa extensia Bitdefender Anti-tracker în browserul web:

1. Selectează **Confidențialitate** din meniul de navigare al interfeței Bitdefender.
2. Selectează fila **Anti-tracker**.
3. Selectează opțiunea **Activare extensie** din dreptul browserului web pentru care dorești să activezi extensia.

Interfața Anti-tracker

Când extensia Bitdefender Anti-tracker este activată, pictograma apare lângă bara de căutare din browserul tău web. De fiecare dată când vizitezi un site web, pe pictogramă vei observa un număr care se referă la trackerele detectate și blocate. Pentru a vizualiza mai multe detalii despre trackerele blocate, apasă pe pictogramă pentru a deschide interfața. În afară de numărul de trackere blocate, poți vizualiza și timpul necesar pentru încărcarea paginii și categoriile din care fac parte trackerele detectate. Pentru a vizualiza lista de site-uri web care sunt urmărite, apasă pe categoria respectivă.

Pentru a dezactiva funcția Bitdefender de blocare a tracker-elor pe site-ul pe care îl accesați în momentul respectiv, selectează opțiunea **Întrerupeți protecția pe acest site**. Această setare se aplică numai atâta timp

cât site-ul este deschis și va reveni automat la starea inițială după ce părăsești site-ul web.

Pentru a permite tracker-elor dintr-o anumită categorie să îți monitorizeze activitatea, selectează activitatea dorită și apoi clic pe butonul corespunzător. Dacă te răzgândești, apasă din nou pe același buton.

Dezactivarea Bitdefender Anti-tracker

Pentru a dezactiva Bitdefender Anti-tracker din browserul web:

1. Deschide browserul web.
2. Efectuează clic pe pictograma de lângă bara de adresă din browserul web.
3. Efectuează clic pe pictograma din colțul din dreapta sus.
4. Utilizează butonul corespunzător pentru dezactivare.
   Pictograma Bitdefender devine gri.

Permiterea urmăririi unui site web

Dacă dorești ca activitatea ta să fie urmărită în timp ce accesezi un anumit site web, poți adăuga adresa acestuia în lista de excepții, după cum urmează:

1. Deschideți browserul web.
2. Efectuează clic pe pictograma de lângă bara de căutare.
3. Apasă pe pictograma din colțul din dreapta sus.
4. Dacă vă aflați pe site-ul web pe care doriți să îl adăugați la excepții, faceți clic pe **Adăugați site-ul web curent la listă**.
   Dacă doriți să adăugați un alt site web, introduceți adresa acestuia în câmpul corespunzător, apoi faceți clic .

4.4.9. Protecție fișiere

Ransomware este un program periculos care atacă sistemele vulnerabile blocându-le și solicită bani pentru a permite utilizatorului să reia controlul asupra sistemului. Acest software periculos acționează inteligent prin afișarea unor mesaje false pentru a panica utilizatorul, solicitându-i să efectueze plata cerută.

Folosind cea mai nouă tehnologie, Bitdefender asigură integritatea sistemului prin protejarea zonelor de importanță critică ale sistemului împotriva atacurilor ransomware, fără a afecta sistemul. Cu toate acestea, este posibil să vrei să-ți protejezi și fișierele personale, cum ar fi documentele, fotografiile sau filmele, împotriva accesării lor de către aplicații nesigure. Cu funcția Bitdefender Protecție fișiere, poți să-ți menții în siguranță fișierele personale și să configurezi ce aplicații ar trebui să aibă dreptul de a efectua modificări asupra fișierelor protejate și ce aplicații nu ar trebui să aibă astfel de drepturi.

Pentru a adăuga ulterior fișiere în mediul protejat:

1. Clic **Protecție** în meniul de navigare din interfața Bitdefender.
2. Selectează fila **Anti-Ransomware**.
3. Selectează **Fișiere protejate** din secțiunea Protecție fișiere.
4. Efectuează clic pe butonul marcat cu semnul plus (+), ce se află sub lista fișierelor protejate. Apoi, selectează fișierul, directorul sau volumul de protejat în cazul în care se încearcă accesarea lor de către programele ransomware.

Pentru a evita încetinirea sistemului, îți recomandăm să adaugi cel mult 30 de directoare sau să salvezi mai multe fișiere într-un singur director.

În mod implicit, directoarele Fotografii, Documente, Desktop și Fișiere descărcate sunt protejate contra atacurilor amenințărilor.

> **Notă**
> Directoarele personalizate pot fi protejate doar pentru utilizatorii curenți. Unitățile, sistemele și fișierele aplicațiilor externe nu pot fi adăugate la mediul de protecție.

Vei fi informat de fiecare dată când o aplicație necunoscută cu un comportament neobișnuit va încerca să modifice fișierele adăugate. Apasă pe **Permite** sau **Blochează** pentru a o adăuga în lista **Administrare aplicații**.

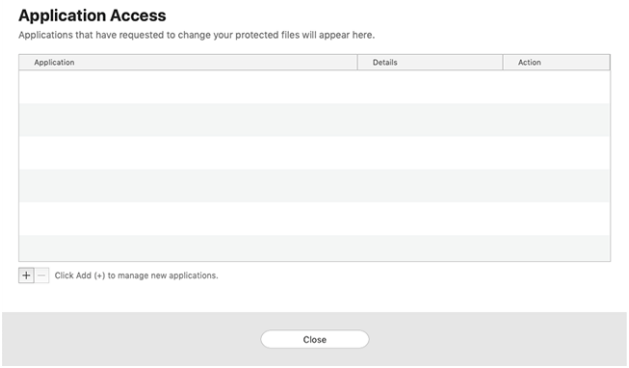
Acces aplicație

Aceste aplicații care încearcă să modifice sau să șteargă fișierele protejate pot fi marcate ca fiind potențial nesigure și adăugate în lista de aplicații blocate. Dacă o astfel de aplicație este blocată și ești sigur că are un comportament normal, îi poți permite accesul urmând acești pași:

1. Clic **Protecție** în meniul de navigare din interfața Bitdefender.
2. Selectează **Anti-Ransomware** fila.
3. Selectează **Acces aplicații** din secțiunea Protecție fișiere.
4. Modifică starea aplicației selectând „Permite” în dreptul aplicației blocate.

Aplicațiile cu starea Permis pot fi setate și pe valoarea Blocat.

Folosește metoda de glisare și fixare (drag&drop) sau efectuează clic pe semnul plus (+) pentru a adăuga în listă mai multe aplicații.



4.4.10. Protecție Time Machine

Protecția Bitdefender Time Machine are rolul unui nivel suplimentar de securitate pentru unitatea ta de backup, inclusiv pentru toate fișierele pe care ai decis să le stochezi acolo, blocând accesul oricărei surse externe. În cazul în care fișierele care se regăsesc pe unitatea Time Machine sunt criptate de un program ransomware, le vei putea recupera fără să plătești recompensa solicitată.

În cazul în care trebuie să restabilești fișiere dintr-un backup Time Machine, accesează pagina de asistență Apple pentru instrucțiuni.

Activarea sau dezactivarea protecției Time Machine

Pentru activa sau dezactiva Protecția Time Machine:

1. Selectează **Protecție** din meniul de navigare al **interfeței Bitdefender**.

2. Selectează **Anti-Ransomware** fila.
3. Activează sau dezactivează opțiunea **Protecție Time Machine**.

4.4.11. Remedierea problemelor

Bitdefender Antivirus for Mac depistează automat o serie de probleme care pot afecta securitatea sistemului și a datelor dvs. și vă informează în acest sens. În acest fel, puteți soluționa riscurile de securitate ușor și rapid.

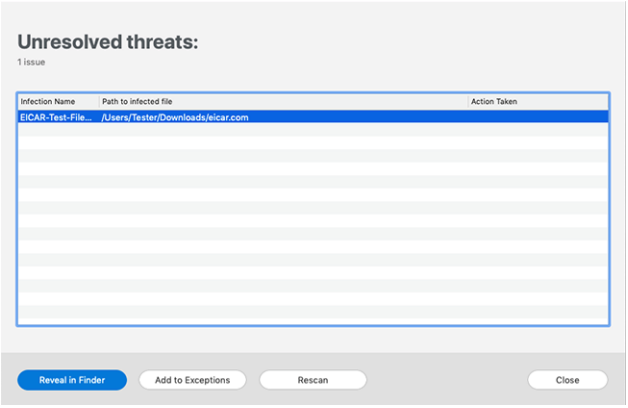
Soluționarea problemelor indicate de Bitdefender Antivirus for Mac constituie un mod rapid și ușor de a asigura protecția optimă a sistemului și a datelor dumneavoastră.

Problemele detectate includ:

- Noua actualizare a informațiilor despre amenințări nu a fost descărcată de pe serverele noastre.
- Au fost detectate amenințări pe sistemul tău și produsul nu le poate dezinfecta automat.
- Protecția în timp real este dezactivată.

Pentru a verifica și soluționa problemele detectate:

1. În cazul în care nu există avertizări din partea Bitdefender, bara de stare este de culoare verde. Atunci când este detectată o problemă de securitate, bara de stare își schimba culoarea în roșu.
2. Verificați descrierea acesteia pentru a obține mai multe informații.
3. Atunci când este detectată o problemă, apasă pe butonul corespunzător pentru a întreprinde o acțiune.



Lista amenințărilor nerezolvate este actualizată după fiecare scanare de sistem, indiferent dacă scanarea se desfășoară automat în fundal sau este inițiată de către tine.

Puteți alege să întreprindeți următoarele acțiuni cu privire la amenințările nesoluționate:

- **Ștergere manuală**. Efectuează această acțiune pentru a elimina manual infecțiile.
- **Adăugare la excepții**. Această acțiune nu este disponibilă pentru amenințările detectate în cadrul arhivelor.

4.4.12. Notificări

Bitdefender menține un jurnal detaliat al evenimentelor legate de activitatea sa pe computerul tău. Ori de câte ori se întâmplă un lucru important pentru securitatea sistemului sau datelor tale, în zona Notificări Bitdefender apare un mesaj nou, ca și când ai primi un e-mail nou în Inboxul tău.

Notificările reprezintă un instrument important pentru monitorizarea și gestionarea protecției Bitdefender. De exemplu, poți verifica cu ușurință dacă actualizarea a fost efectuată cu succes, dacă au fost detectate amenințări sau vulnerabilități pe calculatorul tău, etc. În plus, puteți lua măsuri suplimentare, dacă este cazulsau modifica măsurile luate de Bitdefender.

Pentru a accesa jurnalul de Notificări, efectuează clic pe **Notificări** din meniul de navigare al interfeței Bitdefender. De fiecare dată când se

produce un eveniment critic, se poate observa modificarea contorului pe pictograma .

În funcție de tip și severitate, notificările sunt grupate în:

- Evenimentele **importante** indică problemele principale. Acestea ar trebui verificate imediat.
- Evenimentele de tip **Avertizare** indică probleme care nu sunt de foarte mare importanță. Puteți să le verificați și să le remediați oricând aveți timp.
- Evenimentele de tip **Informații** indică operațiile finalizate cu succes.

Fă clic pe fiecare filă pentru mai multe detalii despre evenimentele generate. Detaliile pe scurt sunt afișate la un singur clic pe titlul fiecărui eveniment, respectiv: o scurtă descriere, acțiunea pe care Bitdefender a întreprins-o atunci când a survenit, precum și data și ora producerii evenimentului. Pot fi setate diverse opțiuni prin intermediul cărora să fie aplicații și alte acțiuni, dacă este necesar.

Pentru a te ajuta să gestionezi cu ușurință evenimentele înregistrate, fereastra Notificări oferă opțiuni de ștergere sau marcare ca citite a tuturor evenimentelor din secțiunea respectivă.

4.4.13. Actualizări

Noi amenințări sunt găsite și identificate în fiecare zi. De aceea este foarte important să îți păstrezi Bitdefender Antivirus for Mac actualizat cu ultimele actualizări care conțin informații despre amenințări.

Actualizarea informațiilor privind amenințările se efectuează din mers, adică fișierele care trebuie actualizate sunt înlocuite progresiv. Astfel, actualizarea nu va afecta funcționarea produsului și, în același timp, se elimină orice vulnerabilitate.

- Dacă Bitdefender Antivirus for Mac este actualizat, poate detecta cele mai recente pericole descoperite și poate curăța fișierele infectate.
- Dacă Bitdefender Antivirus for Mac nu este actualizat, acesta nu va putea detecta și elimina cele mai recente amenințări descoperite de Laboratoarele Bitdefender.

Cererea unei actualizări

Puteți efectua o actualizare la cerere oricând doriți.

Este necesară o conexiune activă la internet pentru a verifica dacă există actualizări disponibile și pentru a le descărca.

Pentru o actualizare la cerere:

1. Faceți clic pe butonul **Acțiuni** din bara de meniu.
2. Selectează **Actualizează baza de date cu informații referitoare la amenințări**.

În mod alternativ, poți solicita o actualizare manuală tastând CMD + U.

Puteți vizualiza progresul actualizării, precum și fișierele descărcate.

Obținerea actualizărilor prin intermediul unui server proxy

Bitdefender Antivirus for Mac se poate actualiza numai prin servere proxy care nu necesită autentificare. Nu este necesară configurarea vreunor setări de program.

Dacă te conectexi la internet prin intermediul unui server proxy ce necesită autentificare, trebuie să treci în mod regulat la o conexiune directă la internet pentru a putea obține actualizările cu privire la informațiile despre amenințări.

Fă upgrade la o versiune nouă

Ocazional, lansăm actualizări de produse pentru a adăuga noi caracteristici și îmbunătățiri sau pentru a remedia anumite probleme legate de produs. Aceste actualizări pot necesita repornirea sistemului pentru a porni instalarea noilor fișiere. În mod implicit, dacă o actualizare necesită repornirea computerului, Bitdefender Antivirus for Mac va continua funcționarea folosind fișierele anterioare, până când reporniți sistemul. În acest caz, procesul de actualizare nu va interfera cu activitatea utilizatorului.

Atunci când este finalizată o actualizare de produs, o fereastră pop-up vă va solicita să reporniți sistemul. Dacă ratați această această notificare, puteți fie să faceți clic pe **Repornește pentru upgrade** din bara de meniu sau să reporniți manual sistemul.

Găsirea informațiilor despre Bitdefender Antivirus for Mac

Pentru a găsi informții despre versiunea Bitdefender Antivirus for Mac pe care ai instalat-o, accesează fereastra **Despre**. Din aceeași

fereastră poți accesa și vizualiza Contractul de abonament și Politica de Confidențialitate și poți vizualiza Licențele cu sursă deschisă.

Pentru a accesa fereastra Despre:

1. Deschideți Bitdefender Antivirus for Mac.
2. Apasă pe Bitdefender Antivirus for Mac din bara de meniu și selectează **Despre Antivirus for Mac**.

4.5. Configurarea preferințelor

Acest capitol include următoarele subiecte:

- Accesarea preferințelor (pagina 177)
- Preferințe de protecție (pagina 177)
- Preferințe avansate (pagina 178)
- Oferte speciale (pagina 178)

4.5.1. Accesarea preferințelor

Pentru deschiderea ferestrei de preferințe a Bitdefender Antivirus for Mac:

- Puteți proceda în oricare dintre următoarele modalități:
  - Clic pe **Preferințe** în meniul de navigare din interfața Bitdefender.
  - Apasă pe Bitdefender Antivirus for Mac din bara de meniu și selectează **Preferințe**.

4.5.2. Preferințe de protecție

Fereastra de setări preferate de protecție îți permite să configurezi abordarea generală de scanare. Puteți configura acțiunile întreprinse în cazul fișierelor infectate și suspecte detectate, precum și alte setări generale.

- **Bitdefender Shield.** Bitdefender Shield oferă protecție în timp real împotriva unei varietăți de amenințări prin scanarea tuturor aplicațiilor instalate, a versiunilor lor actualizate și a fișierelor noi și modificate. Nu îți recomandăm să dezactivezi Bitdefender Shield, însă dacă acest lucru este necesar, asigură-te că acest modul este dezactivat pentru cât mai puțin timp posibil. Dacă Bitdefender Shield este dezactivat, nu vei mai fi protejat împotriva amenințărilor.

- **Scanare doar fișiere noi și modificate.** Selectează această căsuță pentru a configura Bitdefender Antivirus for Mac să scaneze exclusiv fișierele care nu au fost scanate anterior sau care au fost modificate de la ultima scanare.

  Poți alege să nu aplici această setare în cazul scanării personalizate prin drag & drop debifând caseta corespunzătoare.

- **Nu scana conținutul din backupuri.** Selectează această căsuță pentru a exclude fișierele backup de la procesul de scanare. Dacă fișierele infectate sunt restituite ulterior, Bitdefender Antivirus for Mac le va detecta automat și va lua măsurile necesare.

4.5.3. Preferințe avansate

Poți selecta o acțiune generală ce urmează a fi întreprinsă pentru toate problemele și obiectele suspecte identificate în timpul procesului de scanare.

Acțiune pentru obiecte infectate

- **Încearcă dezinfectarea sau mutarea în carantină** - Dacă sunt detectate fișiere infectate, Bitdefender va încerca să le dezinfecteze (să elimine codul periculos) sau să le mute în carantină.
- **Nu întreprinde nicio acțiune** - Nu se va întreprinde nicio acțiune asupra fișierelor detectate.

Acțiune pentru obiecte suspecte

- **Mută fișierele în carantină** - Dacă sunt detectate fișiere suspecte, Bitdefender le va muta în carantină.
- **Nu luați nicio măsură** - Nu se va lua nicio acțiune asupra fișierelor detectate.

4.5.4. Oferte speciale

Atunci când sunt disponibile oferte promoționale, produsul Bitdefender este configurat să te notifice prin intermediul unei ferestre de tip pop-up. Aceasta îți oferă oportunitatea de a beneficia de prețuri avantajoase și de a-ți menține dispozitivele protejate pentru o perioadă mai lungă de timp.

Pentru a activa sau dezactiva notificările privind ofertele speciale:

1. Clic **Preferințe** în meniul de navigare din interfața Bitdefender.

2. Selectează fila **Altele**.
3. Activează sau dezactivează opțiunea **Ofertele mele**.

> **Notă**
> Opțiunea **Ofertele mele** este activată implicit.

4.6. Întrebări frecvente

Cum pot încerca Bitdefender Antivirus for Mac înainte de a solicita un abonament?

Ești un client nou Bitdefender și dorești să încerci produsul nostru înainte de a-l cumpăra. Perioada de evaluare este de 30 de zile și poți utiliza în continuare produsul instalat numai dacă achiziționezi un abonament Bitdefender. Pentru a încerca Bitdefender Antivirus for Mac, trebuie să:

1. Creează-ți un cont Bitdefender urmând acești pași:
   a. Mergi la: https://central.bitdefender.com.
   b. Introdu informațiile solicitate în câmpurile corespunzătoare. Datele furnizate aici vor rămâne confidențiale.
   c. Înainte de a merge mai departe este necesar să îți exprimi acordul cu privire la Condițiile de utilizare. Accesează secțiunea Condiții de utilizare și citește-le cu atenție întrucât conțin termenii și condițiile care îți permit utilizarea Bitdefender.
   Suplimentar, poți accesa și citi Politica de confidențialitate.
   d. Fă clic pe **CREARE CONT**.
2. Descarcă Bitdefender Antivirus for Mac astfel:
   a. Selectează **Dispozitivele mele** panou, apoi faceți clic **INSTALATI PROTECTIA**.
   b. Alegeți una dintre cele două opțiuni disponibile:
      - **Protejați acest dispozitiv**
        i. Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.
        ii. Salvați fișierul de instalare.

- **Protejați alte dispozitive**

  i. Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, faceți clic pe butonul corespunzător.

  ii. Clic **TRIMITE LINK DE DESCARCARE**.

  iii. Introduceți o adresă de e-mail în câmpul corespunzător și faceți clic **TRIMITE EMAIL**.
  Rețineți că linkul de descărcare generat este valabil doar pentru următoarele 24 de ore. Dacă linkul expiră, va trebui să generați unul nou urmând aceiași pași.

  iv. Pe dispozitivul pe care doriți să vă instalați produsul Bitdefender, verificați contul de e-mail pe care l-ați introdus, apoi faceți clic pe butonul de descărcare corespunzător.

c. Rulați produsul Bitdefender pe care l-ați descărcat.

Am deja un cont de activare. Cum adaug valabilitatea acestuia la abonamentul meu?

Dacă ați achiziționat un cod de activare de la unul dintre distribuitorii noștri sau l-ați primit cadou, atunci puteți adăuga disponibilitatea acestuia la abonamentul Bitdefender.

Pentru a activa un abonament folosind un cod de activare, urmați acești pași:

1. Acces Bitdefender Central.
2. Selectează **Abonamentele mele** panou.
3. Apasă pe **COD DE ACTIVARE** butonul, apoi introduceți codul în câmpul corespunzător.
4. Clic **ACTIVATI** a continua.

Extensia este acum vizibilă în contul tău Bitdefender și în produsul tău Bitdefender Antivirus for Mac instalat, în partea din dreapta jos a ecranului.

Jurnalul de scanare indică faptul că există încă o serie de obiecte nesoluționate. Cum le șterg?

Obiectele nesoluționate din jurnalul de scanare pot fi:

- acces restricționat arhive (xar, rar, etc.)
  Soluție: utilizează opțiunea **Arată în Finder** pentru a identifica fișierul și pentru a-l șterge manual. Golește folderul Trash.
- acces restricționat cutii poștale (Thunderbird, etc.)
  Soluție: Utilizați aplicația pentru a șterge înregistrarea care conține fișierul infectat.
- Conținut din back-up-uri
  Soluție: activează opțiunea **Nu scana conținutul backupurilor** din Preferințele privind protecția sau **Adaugă la excepții** fișierele detectate.
  Dacă fișierele infectate sunt restabilite ulterior, Bitdefender Antivirus for Mac le va detecta automat și va acționa în mod corespunzător.

> **Notă**
> Fișierele cu acces restricționat sunt fișiere pe care Bitdefender Antivirus pentru Mac doar le poate deschide, nu le poate modifica.

Unde pot vedea detalii despre activitatea produsului?

Bitdefender păstrează un jurnal al tuturor acțiunilor importante, modificărilor de stare și al altor mesaje critice legate de activitatea sa. Pentru a accesa aceste informații, selectați opțiunea **Notificări** din meniul de navigare al interfeței Bitdefender.

Pot actualiza Bitdefender Antivirus for Mac prin intermediul unui Server Proxy?

Bitdefender Antivirus pentru Mac se poate actualiza numai prin servere proxy care nu necesită autentificare. Nu trebuie să configurați nicio setare a programului.

Dacă vă conectați la internet printr-un server proxy care necesită autentificare, trebuie să treceți la o conexiune directă la internet în mod regulat pentru a obține actualizări ale informațiilor despre amenințări.

Cum dezactivez Bitdefender Antivirus for Mac?

Pentru a elimina Bitdefender Antivirus pentru Mac, urmați acești pași:

1. Deschide o fereastră **Finder**, apoi accesează directorul Aplicații.
2. Deschide directorul Bitdefender și efectuează dublu-clic pe BitdefenderUninstaller.

3. Clic **Dezinstalează** și așteptați finalizarea procesului.
4. Clic **Închide** a termina.

> **Important**
> Dacă apare o eroare, puteți contacta Serviciul pentru clienți Bitdefender, așa cum este descris în Solicitarea ajutorului (pagina 290).

Cum șterg extensiile TrafficLight din browser-ul meu web?

- Pentru a șterge extensiile TrafficLight din Mozilla Firefox, urmați pașii de mai jos:
  1. Accesează **Instrumente** și selectează **Add-on**.
  2. Selectați **Extensii** din coloana din partea stângă.
  3. Selectați extensia și faceți clic pe **Ștergere**.
  4. Reporniți browser-ul pentru finalizarea procesului de ștergere.
- Pentru a șterge extensiile TrafficLight din Google Chrome, urmați pașii de mai jos:
  1. În partea dreaptă de sus, apasă pe **Mai multe** ⋮.
  2. Accesează **Mai multe instrumente** și selectează **Extensii**.
  3. Fă clic pe pictograma **Dezinstalare** 🗑 de lângă extensia pe care dorești să o dezinstalezi.
  4. Efectuează clic pe **Dezinstalare** pentru a confirma procesul de ștergere.
- Pentru a elimina Bitdefender TrafficLight din Safari, urmați pașii de mai jos:
  1. Accesează **Preferințe** sau apasă pe **Command-Comma(,)**.
  2. Selectează **Extensii**.
     Se va afișa o listă cu extensiile instalate.
  3. Selectează extensia Bitdefender TrafficLight, apoi **Dezinstalare**.
  4. Selectează **Dezinstalare** încă o dată pentru a confirma procesul de ștergere.

Când ar trebui să utilizez Bitdefender VPN?

Trebuie să procedezi cu atenție atunci când accesezi, descarci sau încarci conținut pe internet. Ca să fii sigur că ești protejat atunci când navighezi pe web, îți recomandăm să folosești Bitdefender VPN când:

- când dorești să te conectezi la rețele wireless publice
- când dorești să accesezi conținut care în mod normal este restricționat în anumite zone, indiferent dacă ești acasă sau în străinătate
- când dorești să-ți păstrezi confidențialitatea datelor tale personale (nume de utilizator, parole, datele cardului de credit etc.)
- când dorești să-ți ascunzi adresa IP

Bitdefender VPN va avea un impact negativ asupra autonomiei bateriei dispozitivului meu?

Bitdefender VPN este conceput să îți protejeze datele personale, să îți ascundă adresa IP în timp ce ești conectat la rețele wireless nesecurizate și la conținutul cu acces restricționat din anumite țări. Pentru a evita consumarea inutilă a bateriei, îți recomandăm să folosești funcția VPN numai atunci când ai nevoie de ea și să te deconectezi atunci când ești offline.

De ce încetinește viteza de internet atunci când sunt conectat cu Bitdefender VPN?

Bitdefender VPN este conceput să îți ofere o navigare ușoară pe web; totuși, conexiunea ta la internet sau distanța față de serverul la care te conectezi pot cauza o încetinire. În acest caz, dacă nu trebuie neapărat să te conectezi din locația ta la un server îndepărtat (de ex. din SUA sau China), îți recomandăm să permiți Bitdefender VPN să te conecteze automat la cel mai apropriat server, sau să găsești un server mai apropiat de locația ta curentă.

5. SECURITATE MOBILĂ PENTRU ANDROID

5.1. Ce este Bitdefender Mobile Security

Activitățile online, cum ar fi plata facturilor, rezervări pentru vacanță sau achiziționarea de produse și servicii se realizează comod, fără complicații. Însă, la fel ca în cazul multor altor activități pe internet, acestea implică și riscuri mari și, dacă detaliile de securitate sunt ignorate, datele personale pot fi accesate neautorizat. Și ce poate fi mai important decât protejarea datelor stocate în conturile online și pe smartphone-ul personal?

Cu **Bitdefender Mobile Security** ai următoarele beneficii:

- Obții cea mai bună protecție pentru smartphone-ul și tableta ta Android cu un impact minim asupra autonomiei bateriei
- Te protejezi împotriva fraudelor pe mobil bazate pe linkuri
- Ai acces la serviciul nostru VPN securizat pentru o experiență rapidă, anonimă și sigură de navigare pe internet
- Localizează, blochează și șterge de la distanță informațiile de pe dispozitivul tău Android în caz de pierdere sau furt
- Îți verifici contul de e-mail pentru a afla dacă a fost implicat în breșe de securitate a datelor sau scurgeri de date

5.2. Introducere

5.2.1. Cerințe dispozitiv

Bitdefender Mobile Security funcționează pe orice dispozitiv care utilizează Android 5.0 sau orice versiune ulterioară a sistemului de operare. Este necesară o conexiune activă la internet pentru scanarea in-the-cloud a amenințărilor.

5.2.2. Instalarea Bitdefender Mobile Security

- **Din Bitdefender Central**
  - Pe Android
    1. Accesează: https://central.bitdefender.com.

2. Accesează contul tău Bitdefender.
3. Selectați secțiunea **Dispozitivele mele**.
4. Atinge **INSTALARE PROTECȚIE** și apoi **Protejează acest dispozitiv**.
5. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, atinge butonul corespunzător.
6. Vei fi redirecționat către aplicația **Google Play**. În ecranul Google Play, selectează opțiunea de instalare.

- Pe Windows, macOS și iOS
  1. Mergi la: https://central.bitdefender.com.
  2. Conectați-vă la contul dvs. Bitdefender.
  3. Selectează **Dispozitivele mele** panou.
  4. Apasă pe **INSTALARE PROTECȚIE** și apoi pe **Protejează alte dispozitive**.
  5. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, apasă pe butonul corespunzător.
  6. Apasă pe **TRIMITE LINK DE DESCĂRCARE**.
  7. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceeași pași.
  8. Pe dispozitivul pe care dorești să instalezi Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

- **Din Google Play**
  Caută Bitdefender Mobile Security pentru a localiza și instala aplicația. Alternativ, scanați codul QR:

  Înainte de a trece prin pașii de validare, este necesar să accepți Contractul de Abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Mobile Security.

Apasă **CONTINUĂ** pentru a trece la fereastra următoare.

5.2.3. Accesează contul tău Bitdefender

Pentru a utiliza Bitdefender Mobile Security, trebuie să îți conectezi dispozitivul la un cont Bitdefender, Facebook, Google, Microsoft sau Apple, autentificându-te în cont din aplicație. Prima dată când deschizi aplicația, ți se va solicita să te conectezi la un cont.

Dacă ai instalat Bitdefender Mobile Security din contul Bitdefender, aplicația va încerca să se conecteze automat la acel cont

Pentru a-ți asocia dispozitivul unui cont Bitdefender:

1. Introdu adresa de e-mail și parola asociate contului tău Bitdefender în câmpurile corespunzătoare. Dacă nu ai un cont Bitdefender și dorești să îți creezi unul, selectează link-ul corespunzător.
2. Atinge **CONECTARE**.

Pentru a te conecta cu un cont de Facebook, Google sau Microsoft, selectează serviciul dorit din secțiunea Sau conectează-te cu. Vei fi automat redirecționat către pagina de conectare a serviciului selectat. Urmează instrucțiunile pentru a-ți asocia contul cu Bitdefender Mobile Security.

> **Notă**
> Bitdefender nu are acces la informații confidențiale, precum parola contului pe care te autentifici de obicei sau datele personale ale prietenilor și contactelor.

5.2.4. Configurare protecție

Odată ce te-ai conectat cu succes la aplicație, se va afișa fereastra Configurare protecție. Pentru a-ți proteja dispozitivul, îți recomandăm să urmezi acești pași:

- **Status abonament**. Pentru a beneficia de protecția Bitdefender Mobile Security, trebuie să activați produsul prin achiziția unui abonament, care prevede cât timp puteți utiliza produsul. Imediat ce acesta expiră, aplicația nu mai funcționează și nu vă mai protejează dispozitivul.
  Dacă ai un cod de activare, atinge **AM UN COD**, apoi **ACTIVARE**.
  Dacă te-ai autentificat cu un cont Bitdefender nou și nu ai un cod de activare, poți utiliza produsul timp de 14 zile, gratuit.

- **Protecție web**. Dacă dispozitivul tău necesită activarea serviciului Accesibilitate în vederea activării Protecției web, atinge **ACTIVARE**. Vei fi redirecționat către meniul Accesibilitate. Selectează Bitdefender Mobile Security și activează opțiunea corespunzătoare.
- **Scaner malware**. Execută o singură scanare pentru a te asigura că dispozitivul tău nu conține amenințări. Pentru a porni procesul de scanare, atinge **SCANEAZĂ ACUM**.
  Imediat ce începe procesul de scanare, se afișează panoul de control. Aici, poți vedea starea de securitate a dispozitivului tău.

5.2.5. Panou de bord

Atinge pictograma Bitdefender Mobile Security din lista de aplicații a dispozitivului tău pentru a deschide interfața aplicației.

Panoul de control oferă informații despre starea de securitate a dispozitivului tău și, prin intermediul funcției Autopilot, te ajută să îmbunătățești securitatea dispozitivului tău oferindu-ți recomandări cu privire la caracteristicile disponibile.

Panoul de stare din partea de sus a ferestrei te informează cu privire la starea de securitate a dispozitivului tău folosind mesaje explicite și culori sugestive. Dacă Bitdefender Mobile Security nu prezintă avertismente, panoul de stare este verde. Atunci când a fost detectată o problemă de securitate, culoarea panoului de stare devine roșie.

Pentru a-ți oferi o metodă eficientă de operare și o protecție sporită în timp ce desfășori diferite activități, **Bitdefender Autopilot** va acționa ca asistentul tău personal în materie de securitate. În funcție de activitatea pe care o desfășori, Bitdefender Autopilot îți va oferi recomandări contextuale în funcție de modul de utilizare a dispozitivului tău și nevoile tale. Acest lucru te va ajuta să descoperi și să beneficiezi de avantajele furnizate de caracteristicile incluse în aplicația Bitdefender Mobile Security.

De fiecare dată când un anumit proces este în curs de desfășurare sau o funcție necesită răspunsul dumneavoastră, pe Panoul de bord se afișează un card cu mai multe informații și acțiuni posibile.

Poți accesa funcțiile Bitdefender Mobile Security și poți naviga cu ușurință din bara de navigare din partea de jos:

Scaner malware

Îți permite pornirea unei scanări la cerere și activarea scanării dispozitivelor de stocare. Pentru mai multe informații, consultă capitolul Scanare malware (pagina 189).

Protecție web

Asigură o experiență de navigare sigură informându-te cu privire la paginile web potențial periculoase. Pentru mai multe informații, consultă capitolul Protecție web (pagina 192).

VPN

Criptează comunicațiile prin internet, ajutându-te să-ți păstrezi confidențialitatea indiferent de rețeaua la care ești conectat. Pentru mai multe informații, consultați capitolul VPN (pagina 193).

Scam Alert

Te menține în siguranță generând alerte pentru linkurile periculoase pe care le primești prin SMS, aplicații de mesagerie și orice tip de notificare. Pentru informații suplimentare, consultă Scam Alert (pagina 196).

Anti-furt

Vă permite să activați și să dezactivați caracteristicile Anti-Theft, precum și să configurați setările acestei funcții. Pentru mai multe informații, consultă capitolul Funcții Antifurt (pagina 199).

Confidențialitate cont

Verifică dacă s-au produs scurgeri de informații din conturile tale online. Pentru mai multe informații, consultă capitolul Confidențialitate cont (pagina 203).

Blocare aplicații

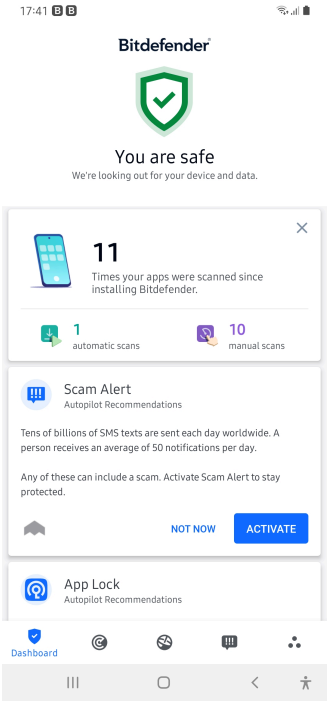
Vă permite să protejați aplicațiile instalate prin setarea unui cod de acces PIN. Pentru mai multe informații, consultă capitolul Blocare Aplicații (pagina 205).

Rapoarte

Păstrează o evidență a tuturor acțiunilor importante, a schimbărilor de stare și a altor mesaje critice legate de activitatea dispozitivului tău. Pentru informații suplimentare, consultă Rapoarte (pagina 209).

WearON

Comunică cu smartwatch pentru a te ajuta să îți găsești telefonul dacă îl rătăcești sau uiti unde l-ai lăsat. Pentru mai multe informații, consultă capitolul WearON (pagina 210).



5.3. Scanare malware

Bitdefender vă protejează dispozitivul și datele împotriva aplicațiilor rău intenționate, utilizând scanarea la instalare și scanarea la cerere.

Interfața Scaner malware oferă o listă cu toate tipurile de amenințări pe care Bitdefender le caută, alături de definițiile acestora. Tot ce trebuie să faci este să selectezi fiecare amenințare pentru a vizualiza definiția aferentă.

Notă

Asigura-te că dispozitivul tău mobil este conectat la internet. Dacă dispozitivul nu este conectat la internet, procesul de scanare nu va porni.

- **Scanare la instalare**
  Ori de câte ori instalezi o aplicație, Bitdefender Mobile Security o scanează automat folosind tehnologia în cloud. Același proces de scanare este inițiat la fiecare actualizare a aplicațiilor instalate.
  Dacă aplicația este depistată a fi rău intenționată, va apărea o alertă care vă va solicita dezinstalarea acesteia. Atinge **Dezinstalare** pentru a merge la ecranul de dezinstalare a aplicației respective.
- **Scanare la cerere**
  Oricând dorești să te asiguri că aplicațiile instalate pe dispozitivul tău sunt sigure în utilizare, poți iniția o scanare la cerere.
  Pentru a porni o scanare la cerere:

  1. Atinge **Scaner malware** din bara de navigare de jos.
  2. Atinge **INIȚIERE SCANARE**.

  > **Notă**
  > Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Scaner Malware. După ce atingi butonul **INIȚIERE SCANARE**, selectează **Permite** pentru următoarele:
  >
  > - Permiți ca **Antivirus** să efectueze și să gestioneze apelurile telefonice?
  > - Permiteți ca **Antivirus** să acceseze fotografii, fișiere media și fișiere stocate pe dispozitivul dumneavoastră?

  Este afișată evoluția scanării și poți opri procesul în orice moment.

În mod implicit, Bitdefender Mobile Security va scana spațiile de stocare internă ale dispozitivului tău, inclusiv orice cartelă SD instalată. În acest fel, orice aplicații periculoase ce se pot afla pe cartelă pot fi detectate înainte de a produce pagube.

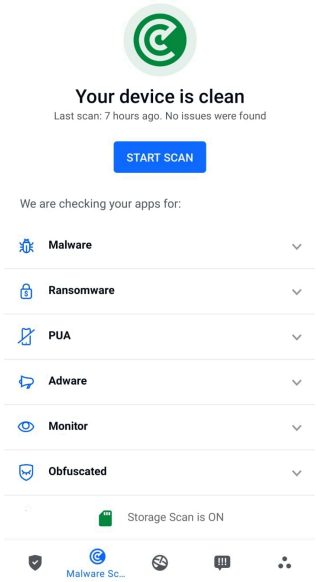
Pentru a dezactiva setarea Scanare dispozitive de stocare:

1. Atinge **Mai multe** din bara de navigare de jos.
2. Atinge **Setări**.
3. Dezactivează selectorul **Scanare dispozitive de stocare** din secțiunea Scaner programe periculoase.

Dacă este detectată orice aplicație rău intenționată, informațiile referitoare la aceasta vor fi afișate și o poți șterge apăsând butonul **DEZINSTALARE**.

Secțiunea Scanare malware afișează starea dispozitivului dumneavoastră. Când dispozitivul este în siguranță, secțiunea este evidențiată cu verde. Când este necesară o scanare a dispozitivului sau există vreo acțiune care necesită răspunsul dumneavoastră, secțiunea este evidențiată cu roșu.

Dacă folosești versiunea de Android 7.1 sau o versiune mai recentă, poți accesa o scurtătură la funcția de Scanare malware astfel încât să poți executa scanările mai rapid, fără a deschide interfața Bitdefender Mobile Security. Pentru a face acest lucru, apasă și menține apăsată pictograma Bitdefender din ecranul principal sau bara de aplicații, apoi selectează pictograma .



5.3.1. Detectarea anomaliilor aplicației

Bitdefender App Anomaly Detection este o tehnologie nouă integrată în Bitdefender Malware Scanner pentru a oferi un nivel suplimentar de protecție prin monitorizarea și detectarea continuă a oricăror comportamente rău intenționate și alertând utilizatorul dacă sunt identificate activități suspecte.

Bitdefender App Anomaly Detection protejează utilizatorii chiar și atunci când aceștia au instalat, fără să știe, o aplicație periculoasă care rulează inactiv pentru o perioadă de timp sau o aplicație aparent de încredere care își întrerupe funcționalitatea și devine necinstită.

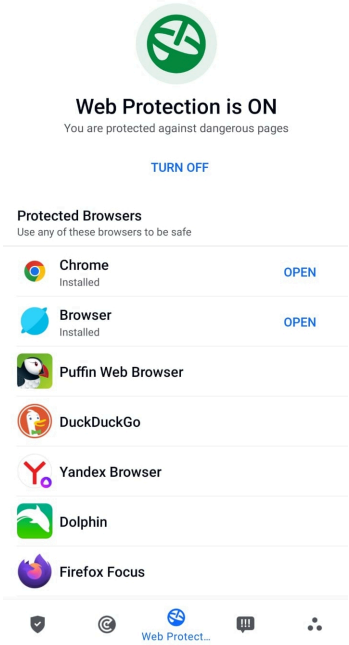
5.4. Protecție web

Caracteristica Protecție Web verifică paginile web pe care le accesezi prin browserul Android implicit, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser și Dolphin, utilizând serviciile în cloud de la Bitdefender.

Notă

Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Securitate web.

Permiteți înregistrarea ca serviciu Accesibilitate și atingeți **PORNIRE** atunci când vi se solicită acest lucru. Atingeți **Antivirus** și activați butonul, apoi confirmați că sunteți de acord cu permisiunea dispozitivului dumneavoastră.



De fiecare dată când accesezi un site bancar, Protecția Web Bitdefender este setată să te notifice să utilizezi serviciul VPN de la Bitdefender. Notificarea apare în bara de stare. Îți recomandăm să utilizezi Bitdefender VPN în timp ce ești conectat la contul tău bancar astfel încât să fii protejat împotriva unor breșe posibile de securitate a datelor.

Pentru a dezactiva notificarea Protecție Web:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Dezactivează comutatorul corespunzător din zona Protecție Web.

5.5. VPN

Cu Bitdefender VPN îșI menții confidențialitatea datelor atunci când te conectezi la rețele wireless nesecurizate în aeroporturi, mall-uri, cafenele sau hoteluri. În acest fel, pot fi evitate situațiile nefericite cum ar fi furtul de date personale sau tentativele de a face IP-ul tău accesibil de către hackeri.

VPS acționează ca tunel între dispozitivul tău și rețeaua la care te conectezi, securizându-ți conexiunea, criptându-ți datele prin criptare la nivel de bancă și ascunzându-ți adresa IP oriunde te-ai afla. Traficul tău este redirecționat prin intermediul unui server separat, ceea ce face ca dispozitivul tău să fie imposibil de identificat între multitudinea de alte dispozitive care folosesc serviciile noastre. Mai mult decât atât, în timp ce ești conectat la internet prin intermediul aplicației VPN, poți accesa conținut care în mod normal este restricționat în anumite zone.

> **Notă**
> Unele țări practică cenzura online, prin urmare utilizarea aplicațiilor VPN pe teritoriul lor este interzisă prin lege. Pentru a evita consecințele legale, este posibil să apară un mesaj de avertizare atunci când încerci să utilizezi aplicația VPN de la Bitdefender pentru prima dată. Prin continuarea utilizării acestei aplicații, confirmi că îți sunt cunoscute reglementările aplicabile din țara respectivă și riscurile la care ai putea fi expus.

Există două moduri de a activa sau dezactiva Bitdefender VPN:

- Apasă **CONECTARE** în cardul VPN din Panoul de bord.
  Se afișează starea Bitdefender VPN.

- Atinge **VPN** din bara de navigare de jos și apoi **CONECTARE**.
  Selectează **CONECTARE** de fiecare dată când dorești să fii protejat atunci când te conectezi la rețele wireless nesecurizate.
  Selectează **DECONECTARE** atunci când vrei să dezactivezi conexiunea.

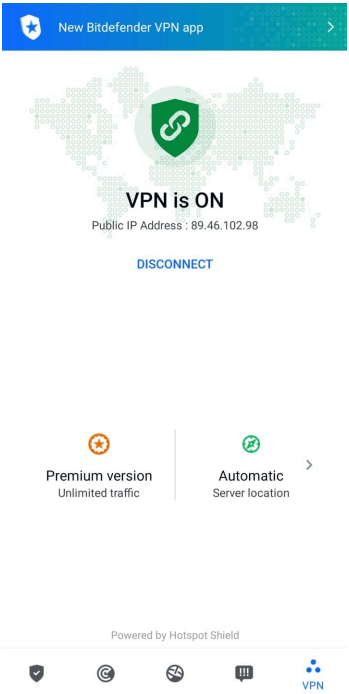
> **Notă**
> Când pornești pentru prima dată VPN-ul ți se cere să permiți Bitdefender să configureze o conexiune VPN care să monitorizeze traficul pe rețea. Apasă **OK** pentru a continua.

Dacă dispozitivul tău utilizează Android 7.1 sau o versiune ulterioară, poți accesa Bitdefender VPN printr-o comandă rapidă, fără să deschizi interfața Bitdefender Mobile Security.

Pentru a face acest lucru, apasă și menține apăsată pictograma Bitdefender din ecranul principal sau bara de aplicații, apoi selectează pictograma .

Pentru a economisi bateria, îți recomandăm să oprești funcția VPN atunci când nu ai nevoie de ea.

Dacă ai un abonament premium și dorești să te conectezi la un anumit server, apasă Locație Server din funcția VPN și apoi selectează locația dorită. Pentru detalii referitoare la abonamentele VPN, accesează



5.5.1. Setări VPN

Pentru o configurare avansată a VPN-ului tău:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.

În zona VPN, poți configura următoarele opțiuni:

- Acces rapid VPN - în bara de stare a dispozitivului tău va apărea o notificare care îți permite să pornești rapid VPN-ul.

- Avertizare rețea Wi-Fi publică - de fiecare dată când te conectezi la o rețea Wi-Fi publică, ești notificat în bara de stare a dispozitivului tău să folosești VPN.

5.5.2. Abonamente

Bitdefender VPN oferă gratuit o cotă de trafic zilnică de 200 MB pe dispozitiv pentru a-ți securiza conexiunea oricând ai nevoie, conectându-te automat la locația optimă a serverului.

Pentru a obține trafic nelimitat și acces nerestricționat la conținutul din întreaga lume alegând o locație de server în funcție de preferințe, efectuează upgrade la versiunea Premium.

Poți să efectuezi oricând un upgrade la versiunea Premium a Bitdefender VPN atingând **Activare Premium** din fereastra VPN.

Abonamentul Bitdefender Premium VPN este independent de abonamentul Bitdefender Mobile Security, ceea ce înseamnă că îl vei putea utiliza cât timp este valabil, indiferent de starea abonamentului tău pentru soluția de securitate. În cazul în care abonamentul Bitdefender Premium VPN expiră, dar abonamentul Bitdefender Mobile Security este încă activ, vei reveni la versiunea gratuită.

Bitdefender VPN este un produs pentru mai multe platforme, disponibil în cadrul produselor Bitdefender compatibile cu Windows, macOS, Android și iOS. După ce faci upgrade la planul Premium, îți vei putea folosi abonamentul pe toate produsele, cu condiția să te conectezi cu același cont Bitdefender.

Notă

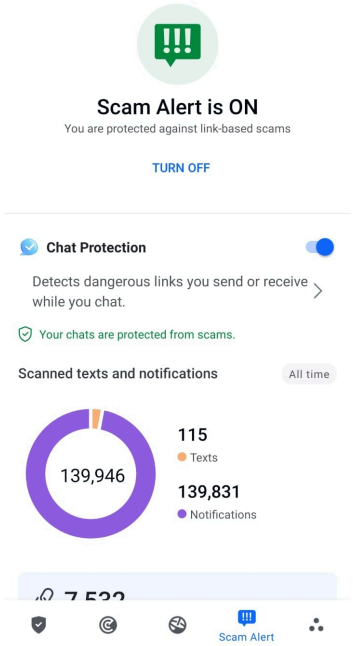
De asemenea, Bitdefender VPN funcționează și ca o aplicație independentă pe toate sistemele de operare compatibile, și anume pe Windows, macOS, Android și iOS.

5.6. Scam Alert

Caracteristica Scam Alert aplică, în prim plan, o serie de măsuri de prevenție, gestionând situații posibil periculoase înainte ca acestea să aibă șansa să devină o problemă, inclusiv cu amenințările malware. Scam Alert monitorizează în timp real toate mesajele SMS și notificările Android primite.

În momentul în care un link periculos ajunge într-un mesaj pe telefonul tău, pe ecran va apărea un avertisment. Bitdefender îți va oferi două opțiuni. Prima este să respingi informația. A doua opțiune este **VIZUALIZARE DETALII**. Aceasta îți oferă mai multe informații despre incident, precum câteva sfaturi esențiale, cum ar fi:

- Nu deschide și nici nu transmite mai departe linkul detectat.
- În cazul mesajelor SMS, ștergeți mesajul, dacă este posibil.
- Blochează expeditorul dacă acesta nu este un contact de încredere.
- Dezinstalează aplicația care trimite linkuri periculoase în notificări.



Notă

Din cauza limitărilor sistemului de operare Android, Bitdefender nu poate șterge mesajele text și nu poate aplica măsuri directe mesajelor SMS sau altor surse de notificări periculoase. Dacă ignori avertismentul Scam Alert și încerci să deschizi linkul periculos, caracteristica Protecție web a Bitdefender îl va detecta automat, împiedicând infectarea dispozitivului tău.

5.6.1. Activarea caracteristicii Scam Alert

Pentru a activa Scam Alert, trebuie să permiți accesul aplicației Bitdefender Mobile Security la mesajele SMS și la sistemul de notificare:

1. Deschide aplicația Bitdefender Mobile Security instalată pe telefonul sau tableta ta Android.
2. În ecranul principal al aplicației Bitdefender, selectează opțiunea **Scam Alert** din bara de navigare de jos, apoi atinge **ACTIVARE**.
3. Atinge butonul **PERMITE**.
4. În lista de acces la notificări, schimbă butonul asociat Bitdefender Security în poziția **PORNIT**.
5. Confirmă acțiunea apăsând pe **PERMITE**.
6. Revino la ecranul Scam Alert și apasă pe **PERMITE** pentru ca Bitdefender să poată scana mesajele SMS pe care le primești.

5.6.2. Protecție chat în timp real

Mesajele chat sunt un mijloc foarte convenabil pentru a ține legătura, însă sunt și cea mai simplă cale prin care linkuri periculoase pot ajunge la tine.

Când caracteristica Protecție chat este activă, protecția oferită de modulul Scam Alert se extinde de la texte și notificări la chaturi, asigurându-se că sunt sigure împotriva atacurilor pe bază de linkuri, detectând linkurile periculoase pe care le trimiți sau primești atunci când comunici prin chat.

Pentru a activa caracteristica Protecție chat:

1. Deschideți aplicația Bitdefender Mobile Security instalată pe telefonul sau tableta dvs. Android.
2. În ecranul principal al aplicației Bitdefender, selectează opțiunea **Scam Alert** din bara de navigare de jos.
3. În partea de sus a filei Scam Alert, vei observa caracteristica Protecție chat. Schimbă butonul corespunzător acesteia în poziția **ACTIVAT**.

Notă

În prezent, caracteristica Protecție Chat este compatibilă cu următoarele aplicații:

- WhatsApp
- Facebook Messenger
- Telegram
- Discord

5.7. Scam Copilot

Această caracteristică este, în esență, un chatbot bazat pe AI, instruit de Bitdefender pentru a detecta diverse scamuri, tentative de phishing, campanii de dezinformare și site-uri web false.

Pentru a activa Scam Copilot:

1. Deschide aplicația Bitdefender Mobile Security. În panoul Meniu principal, se afișează un card care corespunde Scam Copilot. Atinge **Activează**.
2. Activează accesibilitatea la Bitdefender Mobile Security atingând butonul **ACTIVARE**.
3. **Permite** opțiunea de Notificare.

Scam Copilot este acum configurat în mod corespunzător pe dispozitivul tău.

Poți accesa fila dedicată Scam Copilot. Aici vei găsi următoarele opțiuni:

- **Chatbot detecție scamuri:** solicită-i chatbotului să analizeze orice mesaj pe care îl consideri suspect.
- **Asistent prevenție:** te ajută să afli mai multe despre scamuri pentru a deveni expert în identificarea lor.
- **Detecția automată a fraudelor** panoul de stare și control.
- **Filtrare SMS**: filtrează mesajele periculoase direct din aplicația de mesagerie.

5.8. Funcții Antifurt

Bitdefender vă permite să localizați dispozitivul și să preveniți accesul neautorizat la datele dvs.

Tot ce trebuie să faceți este să activați funcția Antifurt pe dispozitiv și, apoi, când este cazul, veți putea accesa **Bitdefender Central** de pe orice browser, de oriunde.

> **Notă**
> Interfața Anti-furt include și un link către aplicația noastră Bitdefender Central în Google Play Store. Poți folosi acest link pentru a descărca aplicația, în cazul în care nu ai făcut deja acest lucru.

Bitdefender Mobile Security oferă următoarele caracteristici Anti-furt:

Localizare de la distanță

Vizualizați locația curentă a dispozitivului dumneavoastră pe Google Maps. Locația este actualizată la fiecare 5 secunde, așadar îl puteți localiza dacă este în mișcare.

Precizia locației depinde de modul în care o poate identifica Bitdefender:

- Dacă funcția GPS este activată pe dispozitiv, locația sa poate fi indicată cu precizie pe o rază de câțiva metri atâta timp cât se află în raza sateliților GPS (mai exact, nu într-o clădire).
- Dacă dispozitivul este înăuntru, locația sa poate fi stabilită la intervale de zeci de metri dacă funcția Wi-Fi este activată și există pe raza sa rețele wireless.
- Altfel, locația va fi stabilită utilizând numai informațiile rețelei mobile, care nu poate oferi o precizie mai mare de câteva sute de metri.

Blocare de la distanță

Blochează ecranul dispozitivului tău și setează un cod PIN numeric pentru deblocarea acestuia.

Ștergere de la distanță

Șterge toate datele tale personale de pe dispozitivul tău înstrăinat.

Expedierea unei alerte pe dispozitiv (Alarmă)

Expediază de la distanță un mesaj care va fi afișat pe ecranul dispozitivului sau declanșați un sunet puternic care să fie redat în difuzorul telefonului.

Dacă pierzi dispozitivul, poți informa persoană care îl găsește cum ți-l poate returna prin afișarea unui mesaj pe ecranul dispozitivului.

Dacă ați rătăcit dispozitivul și se poate să nu fie foarte departe de dumneavoastră (de exemplu, undeva în casă sau în birou), ce metodă ar fi

mai bună pentru a-l găsi decât ca dispozitivul să emită un sunet puternic? Sunetul va fi redat chiar și când dispozitivul se află în modul silențios.

5.8.1. Activarea funcției Antifurt

Pentru a activa funcțiile Antifurt, urmează procesul de configurare din cardul Antifurt disponibil în Panoul de bord.

Alternativ, puteți activa funcția Antifurt urmând pașii de mai jos:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atinge **Anti-furt**.
3. Atinge **ACTIVARE**.
4. Se va lansa următoarea procedură, care te va ajuta să activezi această funcție:

   > **Notă**
   > Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Antifurt.
   >
   > Pentru activare, urmați pașii de mai jos:
   >
   > a. Atinge **Activare Anti-furt** apoi **ACTIVARE**.
   >
   > b. Permite permisiuni pentru **Antivirus** să acceseze locația dispozitivului tău

   a. **Acordă permisiuni de administrator**
   Aceste drepturi sunt esențiale pentru operarea modulului Antifurt și este obligatoriu să fie acordate pentru a putea continua.

   b. **Setează codul PIN al aplicației**
   Pentru a împiedica accesul neautorizat la dispozitivul tău, este necesară configurarea unui cod PIN. La fiecare accesare a dispozitivului tău, este necesar să se introducă mai întâi acest PIN. Ca soluție alternativă, pe dispozitivele care acceptă autentificarea prin intermediul amprentei digitale, se poate utiliza confirmarea pe bază de amprentă digitală în locul codului PIN configurat.
   Același cod PIN este utilizat și de App Lock pentru protejarea aplicațiilor instalate.

   c. **Activează Foto instant**

De fiecare dată când cineva va încerca să îți deblocheze dispozitivul fără succes, în timp ce funcția Instantanee este activată, Bitdefender îi va face o fotografie.

Mai exact, de fiecare dată când se introduce greșit, de trei ori consecutiv, codul PIN, parola, sau confirmarea pe bază de amprentă, care au fost setate de tine pentru a-ți proteja dispozitivul, se va realiza o fotografie cu camera secundară. Imaginea este salvată împreună cu data și ora, precum și motivul realizării, și poate fi vizualizată atunci când deschizi Bitdefender Mobile Security pentru a accesa fereastra Antifurt.

Ca soluție alternativă, poți vizualiza fotografia respectivă din contul tău Bitdefender:

i. Mergi la: https://central.bitdefender.com.

ii. Conectează-te la contul personal.

iii. Selectează **Dispozitivele mele** panou.

iv. Selectează dispozitivul tău Android și apoi fila **Anti-furt**.

v. Atinge ⋮ de lângă **Vezi fotografiile instantanee** pentru a vedea cele mai recente fotografii surprinse.
Sunt salvate doar cele mai recente două fotografii.

Odată ce funcția Anti-Theft este activată, poți activa sau dezactiva comenzile Control web individual din fereastra Anti-Furt prin atingerea opțiunilor corespunzătoare.

5.8.2. Folosirea funcțiilor Anti-Theft din Bitdefender Central

Notă
Toate funcțiile Antifurt solicită ca opțiunea **Date de fundal** să fie activă în setările Utilizare date ale dispozitivului dumneavoastră.

Pentru a accesa caracteristicile Antifurt din contul Bitdefender:

1. Accesează **Bitdefender Central**.
2. Selectează **Dispozitivele mele** panou.
3. În fereastra **DISPOZITIVELE MELE**, selectează cardul de dispozitiv dorit apăsând pe butonul **Vizualizare detalii** corespunzător.
4. Selectați secțiunea **Antifurt**.

5. Apasă pe butonul care corespunde caracteristicii pe care dorești să o utilizezi:
   Localizare - afișează locația dispozitivului tău pe Google Maps.
   Afișează IP - afișează ultima adresă IP a dispozitivului selectat.
   Alertă - tastează un mesaj care să se afișeze pe ecranul dispozitivului tău și/sau setează dispozitivul să genereze o alarmă sonoră.
   Blocare - blochează dispozitivul și setează un cod PIN pentru a-l debloca.
   Ștergere - șterge toate datele din dispozitivul tău.

   > **Important**
   > După ce ștergi un dispozitiv, este oprită funcționarea tuturor funcțiilor Anti-Theft.

5.8.3. Setări Antifurt

Dacă dorești să activezi sau să dezactivezi comenzile la distanță:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Anti furt**.
3. Activează sau dezactivează opțiunile dorite.

5.9. Confidențialitate cont

Funcția Confidențialitate cont Bitdefender detectează dacă s-au produs breșe de securitate a datelor la nivelul conturilor pe care le folosești pentru a efectua plăți și cumpărături online sau pentru a te conecta la diverse aplicații sau site-uri web. Datele care ar putea fi stocate într-un cont includ parole, date de pe cardurile bancare sau informații privind contul bancar și, dacă acestea nu sunt securizate în mod corespunzător, se poate produce un furt de identitate sau o încălcare a confidențialității.

Starea de confidențialitate a unui cont este afișată imediat după validare.

Reverificările automate sunt setate să ruleze în fundal, însă se pot efectua, de asemenea, scanări manuale zilnic.

Se vor afișa notificări de fiecare dată când se descoperă noi scurgeri de informații care implică oricare dintre conturile de e-mail validate.

Pentru a începe să-ți păstrezi în siguranță datele personale:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atinge **Confidențialitate cont**.
3. Selectează **ÎNCEPE UTILIZAREA**.
4. Adresa de e-mail utilizată pentru a-ți crea contul Bitdefender va fi afișată și adăugată automat pe lista de conturi monitorizate.
5. Pentru a adăuga un cont nou, apasă pe **ADĂUGARE CONT** din fereastra Confidențialitate cont și apoi introdu adresa de e-mail.
   Atinge **ADĂUGARE** pentru a continua.
   Bitdefender trebuie să valideze acest cont înainte de a afișa informații private. Prin urmare, se va trimite un e-mail conținând un cod de validare către adresa de e-mail furnizată.
   Verifică-ți inbox-ul și apoi introdu codul primit în secțiunea **Confidențialitate cont** a aplicației. Dacă nu găsești e-mail-ul de validare în Inbox, verifică directorul Spam.
   Se afișează starea de confidențialitate a contului validat.

Dacă se identifică scurgeri de informații pe oricare dintre conturile tale, îți recomandăm să modifici parola acestora cât mai curând posibil. Pentru a crea o parolă puternică și sigură, ia în considerare aceste sfaturi:

- Folosește cel puțin opt caractere.
- Include litere mari și mici.
- Adaugă cel puțin un număr sau simbol, precum #, @, % sau !.

După securizarea unui cont care a fost implicat într-o scurgere de informații, poți confirma modificările marcând încălcările identificate ca fiind Rezolvat(e). Pentru a face acest lucru:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Confidențialitatea contului**.
3. Selectează contul pe care tocmai l-ai securizat.
4. Apasă pe încălcarea față de care ți-ai securizat contul.
5. Apasă **REZOLVAT** pentru a confirma securizarea contului.

După ce toate încălcările de securitate sunt marcate ca fiind **Rezolvate**, contul nu va mai apărea ca fiind implicat într-o încălcare de securitate, cel puțin până când nu se detectează o nouă încălcare de securitate.

Pentru a dezactiva opțiunea de notificare la fiecare scanare automată:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Dezactivează butonul corespunzător din zona Confidențialitate cont.

5.10. Blocare Aplicații

Aplicațiile instalate, cum ar fi e-mail, fotografii sau mesaje, pot conține date personale pe care dorești să le menții confidențiale prin restricționarea selectivă a accesului la acestea.

Funcția de Blocare aplicații te ajută să blochezi accesul nedorit la aplicații prin setarea unui cod de acces PIN. Codul PIN pe care îl configurezi trebuie să aibă cel puțin 4 cifre, însă nu mai mult de 8, și va trebui să îl introduci de fiecare dată când accesezi aplicațiile restricționate selectate.

Poți utiliza autentificarea biometrică (precum confirmarea cu ajutorul amprentei sau prin recunoaștere facială) în locul codului PIN configurat.

5.10.1. Activarea App Lock

Pentru a restricționa accesul la aplicațiile selectate, configurați funcția Blocare aplicații din cardul afișat în Panoul de bord după activarea funcție Antifurt.

Alternativ, poți activa funcția Blocare aplicații urmând pașii de mai jos:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atinge **Blocare aplicație**.
3. Atingeți **PORNIȚI**.
4. Permite accesul la datele privind utilizarea pentru Bitdefender Security.
5. Permite **trimiterea de notificări în timpul utilizării altor aplicații**.
6. Reveniți la aplicație, configurați codul de acces și apoi atingeți **CONFIGURARE PIN**.

> **Notă**
> Acest pas este disponibil numai dacă nu ai configurat anterior codul PIN în secțiunea Antifurt.

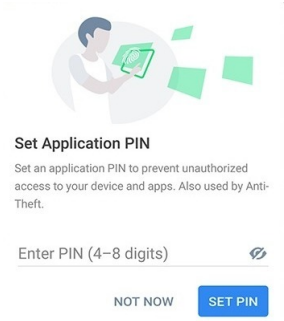
7. Activează opțiunea Fotografiere pentru a putea identifica orice intrus care încearcă să îți acceseze datele.

> **Notă**
> Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Instantanee. Pentru a o activa, permiteți ca **Antivirus** să facă fotografii și să înregistreze clipuri video.

8. Selectează aplicațiile pe care dorești să le protejezi:

Introducerea codului PIN sau aplicarea amprentei greșite de cinci ori consecutiv activează o sesiune de întrerupere a funcționării de 30 de secunde. Astfel, orice încercare de a accesa aplicațiile protejate va fi blocată.

> **Notă**
> Același cod PIN este utilizat și de aplicația Antifurt pentru a te ajuta să îți localizezi dispozitivul.



5.10.2. Mod de blocare

La prima adăugare a unei aplicații la secțiunea Blocare aplicații, apare ecranul Mod blocare aplicații. De aici poți alege momentul în care funcția Blocare aplicații ar trebui să protejeze aplicațiile instalate pe dispozitivul tău.

Poți selecta una dintre următoarele opțiuni:

- **Solicită deblocare de fiecare dată** - de fiecare dată când sunt accesate aplicațiile blocate, va trebui să utilizezi codul PIN sau amprenta pe care le-ai setat.
- **Păstrează deblocat până la oprirea ecranului** - vei putea accesa la aplicațiile până la oprirea ecranului.
- **Blocare după 30 de secunde** - poți ieși și accesa din nou aplicațiile tale deblocate în interval de 30 de secunde.

Dacă dorești să modifici setarea selectată:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Atinge **Solicită deblocare de fiecare dată** din secțiunea Blocare aplicații.
4. Alege opțiunea dorită.

5.10.3. Setări Blocare Aplicații

Pentru o configurare avansată a funcției Blocare aplicații:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.

În zona Blocare aplicații, poți configura următoarele opțiuni:

- **Sugestie aplicații sensibile** - vei primi o notificare de blocare de fiecare dată când instalezi o aplicație sensibilă.
- **Solicită deblocare de fiecare dată** - selectează una dintre opțiunile de blocare și deblocare.
- **Deblocare inteligentă** - păstrează aplicațiile deblocate cât timp ești conectat la rețele Wi-Fi sigure.
- **Randomizare taste** - împiedică citirea codului PIN prin randomizarea poziției cifrelor.

5.10.4. Foto Instant

Cu funcția Bitdefender Foto instant îi poți surprinde pe prietenii sau rudele tale când nu se așteaptă. Astfel, îi poți învăța să nu-și mai arunce privirile curioase prin fișierele tale personale sau aplicațiile pe care le folosești.

Această caracteristică funcționează foarte simplu: de fiecare dată când codul PIN sau amprenta setate pentru a vă proteja aplicațiile sunt introduse greșit de trei ori consecutiv, se realizează o fotografie prin camera frontală. Imaginea este salvată împreună cu data și ora, precum și motivul realizării, și poate fi vizualizată atunci când deschideți Bitdefender Mobile Security pentru a accesa caracteristica Blocare aplicații.

> **Notă**
> Această caracteristică este disponibilă numai pentru telefoanele prevăzute cu cameră frontală.

Pentru a configura Fotografia instant pentru Blocare aplicații:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Activează butonul corespunzător din zona Fotografie instant.

Instantaneele făcute atunci când este introdus codul PIN incorect sunt afișate în fereastra Blocare aplicații și pot fi vizualizate pe întregul ecran.

Alternativ, acestea pot fi vizualizate în contul Bitdefender:

1. Mergi la: https://central.bitdefender.com.
2. Conectați-vă la contul dvs.
3. Selectează secțiunea **Dispozitivele mele**.
4. Selectați dispozitivul dvs. Android, apoi **Anti furt** fila.
5. Atingeți chiar lângă **Verificați-vă instantaneele** pentru a vedea cele mai recente fotografii care au fost făcute.

Sunt salvate doar cele mai recente două fotografii.

Pentru a opri încărcarea instantaneelor în contul tău Bitdefender:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Dezactivează opțiunea **Încărcare fotografii** din secțiunea Fotografie instant.

5.10.5. Deblocare Inteligentă

O metodă ușoară de a evita ca funcția Blocare aplicații să îți solicite să introduci codul PIN sau amprenta de confirmare pentru aplicațiile

protejate de fiecare dată când le accesezi este de a activa opțiunea Deblocare inteligentă.

Cu funcția Deblocare inteligentă poți seta ca fiind sigure rețelele Wi-Fi la care te conectezi de obicei și, atunci când ești conectat la acestea, setările funcției Blocare aplicații vor fi dezactivate pentru aplicațiile protejate.

Pentru a configura funcția Deblocare inteligentă:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Blocare aplicație**.
3. Apasă pe butonul .
4. Apasă butonul de lângă **Deblocare inteligentă** în cazul în care această caracteristică nu este activată.
   Validează folosind amprenta sau codul PIN.
   Prima dată când activezi această caracteristică, va trebui să permiți utilizarea locației. Apasă butonul **PERMITE** și apasă încă o dată **PERMITE**.
5. Atinge **ADAUGĂ** pentru a configura conexiunea Wi-Fi pe care o utilizezi la momentul actual ca fiind sigură.

Dacă te răzgândești, poți dezactiva funcția și rețelele Wi-Fi pe care le-ai setat ca fiind sigure vor fi tratate că fiind nesigure.

5.11. Rapoarte

Funcția Rapoarte păstrează un jurnal detaliat al evenimentelor asociate activității de scanare de pe dispozitivul tău.

La fiecare eveniment relevant pentru securitatea dispozitivului tău un nou mesaj este inclus in Reports.

Pentru a accesa secțiunea Rapoarte:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atinge **Rapoarte**.

În fereastra Rapoarte, sunt disponibile următoarele secțiuni:

- **RAPOARTE SĂPTĂMÂNALE** - aici, ai acces la starea de securitate și la sarcinile efectuate în săptămâna curentă și anterioară. Raportul săptămânii curente este generat în fiecare duminică și vei primi o notificare prin care esti informat cu privire la disponibilitatea acestuia.

Săptămânal va fi afișată o nouă recomandare în această secțiune, astfel, asigura-te ca revii în mod regulat pentru a exploata la maxim aplicația.

Pentru a opri primirea notificărilor de fiecare dată când se generează un raport:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Dezactivează opțiunea **Notificare raport nou** din zona de Rapoarte.

- **JURNAL ACTIVITATE** - de aici, poți verifica informațiile referitoare la activitatea aplicației Bitdefender Mobile Security, de la instalarea acesteia pe dispozitivul tău Android.

  Pentru a șterge jurnalul de activitate disponibil:

  1. Atingeți **Mai mult** pe bara de navigare de jos.
  2. Atingeți **Setări**.
  3. Atinge **Șterge Jurnal de activitate** și apoi apasă pe **ȘTERGE**.

5.12. WearON

Cu funcția Bitdefender WearON, îți poți găsi cu ușurință smartphone-ul, indiferent dacă l-ai lăsat la birou într-o sală de conferințe sau sub o pernă de canapea. Dispozitivul poate fi găsit chiar dacă ai activat modul silențios.

Menține această funcție activată pentru a te asigura că ai întotdeauna smartphone-ul la îndemână.

> **Notă**
> Funcția este compatibilă cu Android 4.3 și Android Wear.

5.12.1. Activarea WearON

Pentru a folosi WearON, nu trebuie decât să te conectezi smartwatch-ul la aplicația Bitdefender Mobile Security și să activezi funcția cu următoarea comandă vocală:

Inițiere:<Unde e telefonul meu>

Bitdefender WearON pune la dispoziție două comenzi:

1. **Alertă telefon**
   Cu funcția Phone Alert îți poți găsi rapid smartphone-ul, ori de câte ori ești prea departe de el.
   Dacă ai smartwatch-ul la tine, acesta detectează automat aplicația de pe telefonul tău și vibrează atunci când ești prea departe de telefon și conexiunea Bluetooth este pierdută.
   Pentru a activa această funcție, deschide Bitdefender Mobile Security, atinge **Global Settings** în meniu și selectează butonul corespunzător în secțiunea WearON.
2. **Scream**
   Găsirea telefonului nu a fost niciodată mai ușoară. Ori de câte ori uitați unde v-ați lăsat telefonul, atingeți comanda Scream de pe ceas pentru a face telefonul să "țipe".

5.13. Despre

Pentru a găsi informații despre versiunea Bitdefender Mobile Security pe care ai instalat-o, pentru a accesa și citi Contractul de abonament și Politica de confidențialitate, precum și pentru a vizualiza Licențele cu sursă deschisă:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Atinge opțiunea dorită în secțiunea Despre.

5.14. Întrebări frecvente

De ce este necesară o conexiune la internet pentru funcționarea Bitdefender Mobile Security?

Aplicația trebuie să comunice cu serverele Bitdefender pentru a determina starea de securitate a aplicațiilor scanate și a paginilor web pe care le vizitați, precum și pentru a primi comenzi de la contul tău Bitdefender, la folosirea funcțiilor Anti-Theft.

Pentru ce este nevoie de fiecare permisiune solicitată de Bitdefender Mobile Security?

- Acces la internet -> utilizat pentru comunicarea în cloud.
- Citire stare și identitate telefon > utilizată pentru a detecta dacă dispozitivul este conectat la internet și pentru a extrage anumite

informații despre dispozitiv necesare pentru a crea o identitate unică pentru comunicarea cu cloud-ul Bitdefender.

- Citire și scriere marcaje în browser > modulul Protecție web șterge site-urile periculoase din istoricul tău de navigare.
- Citire date jurnal > Bitdefender Mobile Security identifică indicii ale activității periculoase din jurnalele Android.
- Locație > este necesară pentru localizarea de la distanță.
- Camera -> necesară pentru funcția Foto instant.
- Stocare > utilizată pentru a permite Scanerului malware să verifice cardul SD.

Cum pot opri trimiterea către Bitdefender a informațiilor despre aplicațiile suspecte?

Bitdefender Mobile Security trimite, în mod automat, rapoarte către serverele Bitdefender cu privire la aplicațiile suspecte pe care le instalezi. Aceste informații sunt esențiale pentru îmbunătățirea detectării amenințărilor și ne poate ajuta să îți oferim o experiență mai bună în viitor. Dacă nu mai dorești să ne transmiți informații despre aplicațiile suspecte:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Dezactivează opțiunea **Detectare în cloud** din zona Scaner programe periculoase.

Unde pot vedea detalii despre activitatea aplicației?

Bitdefender Mobile Security păstrează un jurnal al tuturor acțiunilor importante, modificărilor de stare și al altor mesaje critice legate de activitatea sa. Pentru accesare, vizualizați care este activitatea aplicației:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Rapoarte**.
   În fereastra RAPOARTE SĂPTĂMÂNALE poți accesa rapoartele care sunt generate în fiecare săptămână, iar în fereastra JURNAL ACTIVITATE poți vizualiza informații despre activitatea aplicației tale Bitdefender.

Am uitat codul PIN pe care l-am configurat pentru protejarea aplicației. Ce fac?

1. Acces Bitdefender Central.
2. Selectează **Dispozitivele mele** panou.
3. Atinge cardul dispozitivului dorit și apoi atinge ⋮ din colțul din dreapta sus al ecranului.
4. Selectați **Setări**.
5. Recuperați codul PIN din câmpul **PIN aplicație**.

Cum pot schimba codul PIN pe care l-am configurat pentru Blocare aplicații și Antifurt?

Dacă dorești să modifici codul PIN pe care l-ai configurat pentru Blocare aplicații și Antifurt:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Atinge **COD PIN** de Securitate în secțiunea Antifurt.
4. Tastează codul PIN actual.
5. Tastează noul cod PIN pe care dorești să îl configurezi.

Cum pot dezactiva funcția Blocare aplicații?

Nu există o opțiune de dezactivare a funcției Blocare aplicații, dar o poți opri cu ușurință prin debifarea casetelor de lângă aplicațiile selectate după introducerea codului PIN sau amprentei de validare configurate.

Cum pot configura o altă rețea wireless ca fiind de încredere?

Mai întâi, trebuie să îți conectezi dispozitivul la rețeaua wireless pe care dorești să o configurezi ca fiind sigură. Apoi urmează pașii de mai jos:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Blocare aplicație**.
3. Atinge în colțul din dreapta sus.
4. Atinge **ADĂUGARE** de lângă rețeaua pe care dorești să o configurezi ca fiind sigură.

Cum pot renunța la afișarea fotografiilor realizate de dispozitivele mele?

Pentru a nu mai afișa fotografiile realizate de dispozitivele tale:

1. Acces Bitdefender Central.
2. Atinge în partea dreaptă de sus a ecranului.
3. Atinge **Setări** din meniul vertical.
4. Dezactivează opțiunea **Afișează/nu mai afișa instantanee realizate pe dispozitivele tale**.

Cum pot efectua cumpărături online în siguranță?

Cumpărăturile online prezintă riscuri mari atunci când sunt ignorate anumite detalii. Pentru a nu deveni victima unei fraude, îți recomandăm următoarele:

- Păstrează securitatea ta actualizată.
- Trimite plăți online numai dacă este asigurată protecția cumpărătorului.
- Folosește un VPN atunci când te conectezi la internet prin intermediul unor rețele wireless publice sau nesecurizate.
- Atenție la parolele atribuite conturilor tale online. Acestea trebuie să fie puternice și să includă litere mari și mici, numere și simboluri (@, !, %, #, etc.).
- Asigură-te că informațiile sunt trimise prin intermediul unor conexiuni sigure. Extensiile site-urilor online trebuie să fie HTTPS://, nu HTTP://.

Când ar trebui să utilizez Bitdefender VPN?

Trebuie să procedezi cu atenție atunci când accesezi, descarci sau încarci conținut pe internet. Ca să fii sigur că ești protejat atunci când navighezi pe web, îți recomandăm să folosești Bitdefender VPN când:

- când dorești să te conectezi la rețele wireless publice
- când dorești să accesezi conținut care în mod normal este restricționat în anumite zone, indiferent dacă ești acasă sau în străinătate
- când dorești să-ți păstrezi confidențialitatea datelor tale personale (nume de utilizator, parole, datele cardului de credit etc.)
- când dorești să-ți ascunzi adresa IP

Bitdefender VPN va avea un impact negativ asupra autonomiei bateriei dispozitivului meu?

Bitdefender VPN este conceput să îți protejeze datele personale, să îți ascundă adresa IP în timp ce ești conectat la rețele wireless nesecurizate

și la conținutul cu acces restricționat din anumite țări. Pentru a evita consumarea inutilă a bateriei, îți recomandăm să folosești funcția VPN numai atunci când ai nevoie de ea și să te deconectezi atunci când ești offline.

De ce încetinește viteza de internet atunci când sunt conectat cu Bitdefender VPN?

Bitdefender VPN este conceput să îți ofere o navigare ușoară pe web; totuși, conexiunea ta la internet sau distanța față de serverul la care te conectezi pot cauza o încetinire. În acest caz, dacă nu trebuie neapărat să te conectezi din locația ta la un server îndepărtat (de ex. din SUA sau China), îți recomandăm să permiți Bitdefender VPN să te conecteze automat la cel mai apropriat server, sau să găsești un server mai apropiat de locația ta curentă.

Pot schimba contul Bitdefender asociat dispozitivului meu?

Da, puteți schimba cu ușurință contul Bitdefender asociat dispozitivului dvs. urmând pașii de mai jos:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atinge adresa ta de e-mail.
3. Atinge **Deconectează-te de la contul tău**. Dacă a fost configurat un cod PIN, ți se solicită să îl introduci.
4. Confirmați alegerea dvs.
5. Introdu adresa e-mail și parola contului tău în câmpurile corespunzătoare și selectează **AUTENTIFICARE**.

Ce impact va avea Bitdefender Mobile Security asupra dispozitivului meu în materie de performanțe și baterie?

Impactul este extrem de redus. Aplicația rulează numai atunci când este absolut necesar – inclusiv la instalare și în timpul utilizării interfeței – sau atunci când efectuezi o verificare de siguranță. Bitdefender Mobile Security nu rulează în fundal atunci când efectuați apeluri telefonice, când scrieți mesaje sau vă jucați.

Ce înseamnă Administratorul dispozitivului?

Administratorul dispozitivului este o funcție Android care oferă aplicației Bitdefender Mobile Security permisiunile necesare pentru a efectua anumite sarcini de la distanță. În lipsa acestor drepturi de acces, blocarea

de la distanță nu ar funcționa, iar caracteristica de ștergere a datelor de pe dispozitiv nu ar putea elimina datele tale în totalitate. Dacă dorești să ștergi aplicația, asigură-te că retragi aceste drepturi de acces înainte de a încerca dezinstalarea accesând **Setări > Securitate > Selectare administratori dispozitiv**.

Cum să remediați eroarea "Lipsă Token Google" care apare la autentificarea din Bitdefender Mobile Security.

Această eroare apare atunci când dispozitivul dumneavoastră nu este asociat cu un cont Google sau este asociat cu un cont, dar o problemă temporară împiedică conectarea la Google. Încercați una dintre următoarele soluții:

- Accesează Setări > Aplicații > Gestionare aplicațiile > Bitdefender Mobile Security și apasă pe **Ștergere date**. Apoi încearcă din nou să te conectezi.
- Asigura-te că dispozitivul tău este asociat cu un cont Google.
  Pentru a verifica, accesează Setări > Conturi și sincronizare și vezi dacă apare vreun cont Google în secțiunea **Gestionare conturi**. Dacă nu apare niciun cont, adaugă contul tău, repornește dispozitivul și încearcă să te conectezi din nou în Bitdefender Mobile Security.
- Repornește dispozitivul și încearca să te autentifici din nou.

În ce limbi este disponibil Bitdefender Mobile Security?

Bitdefender Mobile Security este disponibil în prezent în următoarele limbi:

- Portugheză braziliană
- Cehă
- Olandeză
- Engleză
- Franceză
- Germană
- Greacă
- Maghiară
- Italiană

- Japoneză
- Coreană
- Poloneză
- Portugheză
- Română
- Rusă
- Spaniolă
- Suedeză
- Thailandeză
- Turcă
- Vietnameză

În versiunile ulterioare vor fi adăugate și alte limbi. Pentru a modifica limba în care se afișează interfața Bitdefender Mobile Security, accesează setările**Limbă și tastatură** ale dispozitivului tău și setează limba pe care dorești să o utilizezi.

6. SECURITATE MOBILĂ PENTRU IOS

6.1. Ce este Bitdefender Mobile Security for iOS

Activitățile online, cum ar fi plata facturilor, rezervări pentru vacanță sau achiziționarea de produse și servicii se realizează comod, fără complicații. Însă, la fel ca în cazul multor altor activități pe internet, acestea implică și riscuri mari și, dacă detaliile de securitate sunt ignorate, datele personale pot fi accesate neautorizat. Și ce poate fi mai important decât protejarea datelor stocate în conturile online și pe smartphone-ul personal?

Bitdefender Mobile Security for iOS îți permite:

- Cea mai eficientă protecție împotriva amenințărilor cu cel mai mic impact asupra bateriei
- Protejezi datele cu caracter personal: parolele, adresa și informațiile financiare
- Verifică ușor securitatea telefonului pentru a detecta și a remedia configurațiile greșite care l-ar putea expune la riscuri
- Eviți expunerea accidentală a datelor și utilizarea necorespunzătoare a tuturor aplicațiilor instalate
- Scanează-ți dispozitivul pentru a obține setări optime de securitate și confidențialitate
- Obții informații cu privire la activitatea ta online și istoricul incidentelor prevenite
- Verifică-ți conturile online pentru a detecta breșe de securitate a datelor sau scurgeri de date
- Criptezi traficul de pe internet cu VPN-ul inclus

Bitdefender Mobile Security for iOS este un produs gratuit care trebuie activat prin intermediul unui cont Bitdefender. Însă, anumite funcționalități importante ale Bitdefender, precum modulul Protecție web, pot fi accesate de către utilizatori doar prin plata unui abonament.

6.2. Introducere

6.2.1. Cerințe dispozitiv

Bitdefender Mobile Security for iOS este compatibil cu orice dispozitiv care rulează iOS 12 sau o versiune ulterioară a sistemului de operare și necesită o conexiune activă la internet pentru a fi activat și pentru a detecta dacă la nivelul conturilor tale online s-a produs o scurgere de date.

6.2.2. Instalare Bitdefender Mobile Security for iOS

- **Din Bitdefender Central**
  - Pe iOS
    1. Accesează **Bitdefender Central**.
    2. Selectați secțiunea **Dispozitivele mele**.
    3. Atinge **INSTALARE PROTECȚIE** și apoi **Protejează acest dispozitiv**.
    4. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, atinge butonul corespunzător.
    5. Vei fi redirecționat către aplicația **App Store**. În ecranul App Store, selectează opțiunea de instalare.
  - Pe Windows, macOS, Android
    1. Acces Bitdefender Central.
    2. Selectează **Dispozitivele mele** panou.
    3. Apasă pe **INSTALARE PROTECȚIE** și apoi pe **Protejează alte dispozitive**.
    4. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, apasă pe butonul corespunzător.
    5. Apasă pe **TRIMITE LINK DE DESCĂRCARE**.
    6. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceeași pași.

7. Pe dispozitivul pe care dorești să instalezi Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

- **Din App Store**
  Caută Bitdefender Mobile Security pentru iOS pentru a localiza și instala aplicația.

Când deschizi pentru prima dată aplicația, se va afișa o fereastră ce conține detalii despre caracteristicile produsului. Accesează opțiunea Înainte de a începe pentru a continua cu următoarea fereastră.

Înainte de a trece prin pașii de validare, este necesar să accepți Contractul de Abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Mobile Security pentru iOS.

Selectează **Continuă** pentru a trece la fereastra următoare.

6.2.3. Accesează contul tău Bitdefender

Pentru a utiliza Bitdefender Mobile Security for iOS, trebuie să îți conectezi dispozitivul la un cont Bitdefender, Facebook, Google, Microsoft sau Apple, autentificându-te în cont din aplicație. Prima dată când deschizi aplicația, ți se va solicita să te conectezi la un cont.

Pentru a-ți asocia dispozitivul unui cont Bitdefender:

1. Introdu în câmpul corespunzător adresa de e-mail asociată contului tău Bitdefender, apoi selectează opțiunea **ÎNAINTE**. Dacă nu ai încă un cont Bitdefender și dorești să-ți creezi unul, accesează linkul corespunzător și apoi urmează instrucțiunile de pe ecran până când contul este activat.
   Pentru a te conecta cu un cont de Facebook, Google, Apple sau Microsoft, selectează serviciul dorit din secțiunea **Sau conectează-te cu**. Vei fi automat redirecționat către pagina de conectare a serviciului selectat. Urmează instrucțiunile pentru a-ți asocia contul cu Bitdefender Mobile Security for iOS.

> **Notă**
> Bitdefender nu are acces la informații confidențiale, precum parola contului pe care te autentifici de obicei sau datele personale ale prietenilor și contactelor.

2. Introdu parola și apoi selectează **AUTENTIFICARE**.

De aici poți accesa și Politica de confidențialitate a Bitdefender.

6.2.4. Panou de bord

Atinge pictograma Bitdefender Mobile Security for iOS din lista de aplicații a dispozitivului tău pentru a deschide interfața aplicației.

Prima dată când accesezi aplicația, ți se va solicita să permiți Bitdefender să-ți trimită notificări. Selectează opțiunea **Permite** pentru a rămâne informat de fiecare dată când Bitdefender trebuie să-ți comunice ceva care are legătură cu aplicația ta. Pentru administrarea notificărilor Bitdefender, accesează Setări > Notificări > Mobile Security.

Pentru a avea acces la secțiunea de care ai nevoie, accesează pictograma corespunzătoare din partea de jos a ecranului.

Protecție web

Rămâi în siguranță în timp ce navighezi pe internet și oricând aplicațiile mai puțin securizate încearcă să acceseze domenii nesigure. pentru informații suplimentare, accesează Protecție web (pagina 226).

VPN

Protejează-ți confidențialitatea indiferent de rețeaua la care te conectezi menținând criptată conexiunea la internet. Pentru informații suplimentare, accesează VPN (pagina 228).

Confidențialitate cont

Află dacă au fost sau nu accesate neautorizat conturile tale de e-mail. Pentru mai multe informații, consultați capitolul Confidențialitate cont (pagina 231).

Pentru a vizualiza opțiuni suplimentare, accesează pictograma ••• de pe dispozitivul tău când te afli pe pagina principală a aplicației. Vor apărea următoarele opțiuni:

- **Restabilire achiziții** - din această secțiune poți restabili abonamentele anterioare achiziționate folosind contul tău iTunes.
- **Setări** - din această secțiune ai acces la:
  - **Setări VPN**
    - **Contract** - aici poți citi condițiile conform cărora poți utiliza serviciul Bitdefender VPN. Dacă selectezi **Nu mai sunt de acord**, nu vei putea utiliza Bitdefender VPN cel puțin până când nu apeși **Sunt de acord**.
    - **Avertisment rețea Wi-Fi deschisă** - poți activa sau dezactiva notificarea produsului care se afișează de fiecare dată când te conectezi la o rețea Wi-Fi nesecurizată.
      Scopul acestei notificări este de a te ajuta să-ți menții confidențialitatea și securitatea datelor tale folosind Bitdefender VPN.
  - **Setări Protecție web**
    - **Contract** - aici poți citi condițiile conform cărora poți utiliza serviciul Bitdefender Protecție web. Dacă selectezi **Nu mai sunt de acord**, nu vei putea utiliza Bitdefender VPN cel puțin până când nu apeși **Sunt de acord**.
    - **Activare notificări Protecție web** - Primești notificări care te anunță că serviciul Protecție web poate fi activat după finalizarea unei sesiuni VPN.
  - **Rapoarte produs**
- **Feedback** – de aici poți lansa clientul de e-mail implicit pentru a ne trimite feedback privind aplicația.
- **Detalii App** - de aici poți accesa informațiile privind versiunea instalată și Contractul de abonament, Politica de confidențialitate și conformitatea cu licențele open-source.

6.3. Scanare

Cu ajutorul Bitdefender Mobile Security for iOS, îți poți scana dispozitivul pentru a identifica orice vulnerabilități în ceea ce privește securitatea și amenințări posibile de pe dispozitivul tău. Efectuarea scanării va verifica următoarele:

- **Versiunea sistemului de operare:** Se verifică versiunea iOS pentru cele mai recente actualizări.
- **Parola/Date biometrice:** verifică nivelul de securitate când vine vorba de accesarea dispozitivului tău.
- **Protecție web:** verifică starea modulului Protecție web
- **Confidențialitate cont:** verifică prezența conturilor monitorizate enumerate în modulul Confidențialitate cont.
- **Scanare Wi-Fi:** verifică nivelul de securitate al rețelei la care ești conectat.

Starea protecției este determinată după ce efectuezi o scanare manuală.

După ce efectuezi prima scanare, vei fi întâmpinat de recomandările Autopilotului Bitdefender. Acesta este consilierul tău de securitate, care îți oferă recomandări contextuale pe baza modului de utilizare și necesităților dispozitivului tău. Astfel, vei beneficia de tot ce îți poate oferi aplicația ta.

> **Notă**
> Atunci când accesezi prima dată aplicația, ți se va solicita să efectuezi o scanare.

6.4. Scam Alert

Funcția de Scam Alert disponibilă în Bitdefender Mobile Security pentru iOS protejează în mod proactiv utilizatorii Apple de escrocherii de tip phishing. Scam Alert pentru iOS include două straturi de protecție care monitorizează înșelăciunile livrate prin mesaje SMS/MMS și invitații din calendar:

- **Filtru de mesaje text (SMS, MMS)**
  Această caracteristică identifică și filtrează mesajele SMS și MMS nedorite.
  Un SMS/MMS rău intenționat (Short Message Service/Multimedia Messaging Service) se referă la un tip de mesaj trimis către dispozitive mobile cu intenții dăunătoare. Aceste mesaje sunt concepute pentru a exploata vulnerabilități, pentru a înșela destinatarii sau pentru a provoca daune dispozitivului, informațiilor personale sau securității țintei.

- **Calendar Invite Link Scanner**
  Această funcție detectează calendarele spam și evenimentele care conțin linkuri periculoase. Virusul calendarului este un tip de spam care afectează aplicația Calendar a iPhone-ului tău, care poate fi enervant și potențial periculoasă:
  - Primești invitații de calendar sau notificări de evenimente nedorite atunci când accepți din greșeală o invitație de calendar falsă trimisă la adresa ta de e-mail de către hackeri sau spammeri.
  - Când faceți clic pe linkul din invitație, vă abonați fără să știți la calendarul expeditorului, ceea ce îi permite acestuia să vă trimită mai multe evenimente spam.
  - Evenimentele de spam pot conține link-uri sau atașamente care ar putea să vă conducă către pagini de phishing sau alte amenințări cibernetice dacă le deschideți.

6.4.1. Cum se configurează Scam Alert

Pentru a activa Scam Alert, trebuie să acordați aplicației Bitdefender Mobile Security acces la notificările din calendar și la mesajele SMS:

Cum să activați filtrarea SMS:

Pentru ca Bitdefender să înceapă să filtreze mesajele, trebuie să activați manual opțiunea Filtrați expeditorii necunoscuți din setările aplicației Mesaje:

1. Deschide **Setări** aplicația pe iPhone sau iPad.
2. Derulați în jos și selectați **Mesaje** dinn listă.
3. Apasă pe **Necunoscut sau spam** secțiune.
4. Comutati **Filtrați expeditorii necunoscuți** pe poziția pornit.
5. Selectați **Securitate mobilă** în secțiunea Filtrare SMS și apoi alegeți **Permite**.

Bitdefender va putea acum să filtreze mesajele nedorite de pe iPhone/iPad.

> **Notă**
> Din cauza restricțiilor iOS, filtrarea SMS-urilor Bitdefender poate fi utilizată numai pentru mesajele SMS și MMS care provin de la persoane pe care nu le-ați salvat în contacte. Aceasta înseamnă că nu va filtra mesajele de la persoane aflate deja în lista de contacte sau mesajele iMessage de la nimeni.

Cum să activați scanarea calendarului:

1. Deschide aplicația **Bitdefender Mobile Security** instalată pe iPhone sau iPad.
2. Du-te la opțiunea **Scam Alert** din bara de navigare de jos și apăsați pe **Configurați acum**.
3. Atingeți **Continua**, apoi atingeți **Permite**.
4. Alege **OK** pentru a acorda Bitdefender acces la calendarul dvs. O scanare a calendarului va începe imediat.

6.5. Scam Copilot

Această caracteristică este, în esență, un chatbot bazat pe AI, instruit de Bitdefender pentru a detecta diverse scamuri, tentative de phishing, campanii de dezinformare și site-uri web false.

Pentru a activa Scam Copilot:

1. Deschide aplicația Bitdefender Mobile Security. În panoul Meniu principal, se afișează un card care corespunde Scam Copilot. Atinge **Activează**.
2. Va trebui să activezi funcția Filtrare SMS conform instrucțiunilor de mai jos:
   a. Deschide **Setări** pe dispozitivul tău.
   b. Selectează **Mesaje** din listă.
   c. Selectează **Necunoscut și Spam**.
   d. Activează **Filtrare expeditori necunoscuți**.
   e. Selectează **Mobile Security** în fila Filtrare SMS.
3. Când ai terminat, apasă pe **Continuare**.

4. Activează Scanare calendar. O fereastră pop-up va apărea pe ecran la scurt timp după ce apeși pe **Activare**. Apasă pe **Permite acces total**.

Scam Copilot este acum configurat în mod corespunzător pe dispozitivul tău.

Poți accesa fila dedicată Scam Copilot. Aici vei găsi următoarele opțiuni:

- **Chatbot detecție scamuri:** solicită-i chatbotului să analizeze orice mesaj pe care îl consideri suspect.
- **Asistent prevenție:** te ajută să afli mai multe despre scamuri pentru a deveni expert în identificarea lor.
- **Detecția automată a fraudelor** panoul de stare și control.
- **Filtrare SMS**: filtrează mesajele periculoase direct din aplicația de mesagerie.

6.6. Protecție web

Modulul Protecție web Bitdefender asigură o experiență sigură de navigare trimițându-ți alerte cu privire la paginile web potențial periculoase și încercările de accesare de către aplicațiile instalate mai puțin securizate a unor domenii nesigure.

Atunci când o adresă URL face trimitere la un site web cunoscut pentru conținutul său de tip phishing sau fraudulos sau la conținut periculos, cum ar fi spyware sau viruși, pagina web respectivă este blocată și se afișează o alertă. Același lucru se întâmplă atunci când aplicațiile instalate încearcă să acceseze domenii periculoase.

> **Important**
> Dacă te afli într-o zonă în care utilizarea unui serviciu VPN este restricționată prin lege, funcționalitatea Protecție web nu va fi disponibilă.

Pentru a activa Protecția web:

1. Atinge pictograma din partea de jos a ecranului.
2. Apasă **Sunt de acord**.
3. Activează butonul Protecție web.

Notă

Prima dată când activezi modulul Protecție web, este posibil să ți se solicite să permiți Bitdefender să creeze configurații VPN care să monitorizeze traficul de rețea. Selectează **Permite** pentru a continua. Dacă a fost setată o metodă de autentificare (prin amprentă sau cod PIN) pentru a-ți proteja smartphone-ul, trebuie să o folosești. Pentru a putea detecta accesul la domeniile nesigure, modulul Protecție web funcționează împreună cu serviciile VPN.

Important

Caracteristica Protecție web și serviciul VPN nu pot funcționa simultan. Atunci când una dintre acestea este activată, cealaltă (dacă este activă în acel moment) va fi dezactivată.

6.6.1. Alerte Bitdefender

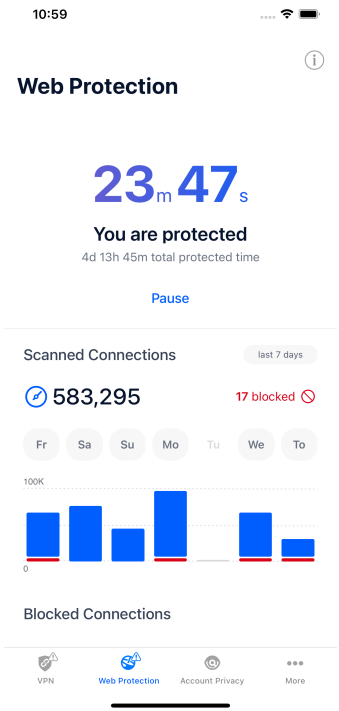
Ori de câte ori încerci să accesezi un site clasificat ca fiind nesigur, site-ul respectiv este blocat. Pentru a te informa despre acest eveniment, vei primi o notificare din partea Bitdefender în Centrul de notificări, precum și în browser. Pagina de avertizare conține informații precum adresa URL a site-ului și amenințarea detectată. Trebuie să decizi cum dorești să se procedeze în continuare.

De asemenea, vei primi o notificare în Centrul de notificări ori de câte ori o aplicație mai puțin sigură încearcă să acceseze domenii care nu sunt de încredere. Accesează notificarea respectivă pentru a fi redirecționat către fereastra în care poți decide cum dorești să procedezi în continuare.

Următoarele opțiuni sunt disponibile pentru ambele situații:

- Părăsește site-ul web respectiv selectând **REVENIRE LA O PAGINĂ SIGURĂ**.
- Accesează site-ul, în ciuda avertizării, selectând notificarea respectivă și apoi **Vreau să accesez pagina**.

Confirmă alegerea.



6.7. VPN

Cu Bitdefender VPN îşi menţii confidenţialitatea datelor atunci când te conectezi la reţele wireless nesecurizate în aeroporturi, mall-uri, cafenele sau hoteluri. În acest fel, pot fi evitate situaţiile nefericite cum ar fi furtul de date personale sau tentativele de a face IP-ul tău accesibil de către hackeri.

VPN acţionează ca tunel între dispozitivul tău şi reţeaua la care te conectezi, securizându-ţi conexiunea, criptându-ţi datele prin criptare de talie militară şi ascunzându-ţi adresa IP oriunde te-ai afla. Traficul tău este redirecţionat prin intermediul unui server separat, ceea ce face ca dispozitivul tău să fie imposibil de identificat de către ISP între multitudinea de alte dispozitive care folosesc serviciile noastre. Mai mult decât atât, în timp ce eşti conectat la internet prin intermediul Bitdefender Password Manager, poţi accesa conţinut care în mod normal este restricţionat în anumite zone.

> **Notă**
> Unele țări practică cenzura online, prin urmare utilizarea aplicațiilor VPN pe teritoriul lor este interzisă prin lege. Pentru a evita consecințele legale, este posibil să apară un mesaj de avertizare atunci când încerci să utilizezi aplicația VPN de la Bitdefender pentru prima dată. Prin continuarea utilizării acestei aplicații, confirmi că îți sunt cunoscute reglementările aplicabile din țara respectivă și riscurile la care ai putea fi expus.

Activează Bitdefender VPN:

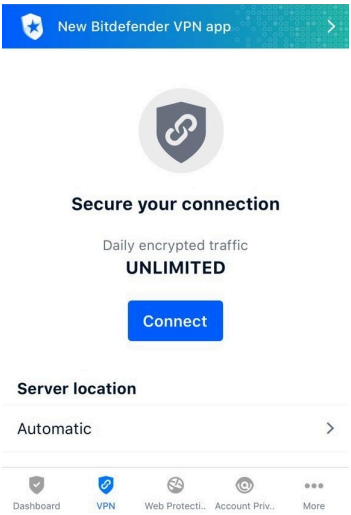
1. Apasă pe pictograma din partea de jos a ecranului.
2. Selectează **Conectare** de fiecare dată când dorești să fii protejat atunci când te conectezi la rețele wireless nesecurizate.
   Selectează **Deconectare** atunci când vrei să dezactivezi conexiunea.

> **Notă**
> Prima dată când activezi modulul VPN, ți se va solicita să permiți Bitdefender să creeze configurații VPN care să monitorizeze traficul de rețea. Selectează **Permite**, pentru a continua. Dacă a fost setată o metodă de autentificare (prin amprentă sau cod PIN) pentru a-ți proteja smartphone-ul, trebuie să o folosești.

Când VPN este activat, pictograma VPN apare pe bara de stare.

Pentru a economisi bateria, îți recomandăm să oprești funcția VPN atunci când nu ai nevoie de ea.

Dacă ai un abonament premium și dorești să te conectezi la un anumit server, selectează Automat în interfața VPN și alege locația dorită. Pentru informații suplimentare privind abonamentele VPN, consultă Abonamente (pagina 230).



6.7.1. Abonamente

Bitdefender VPN oferă gratuit o cotă de trafic zilnică de 200 MB pe dispozitiv pentru a-ți securiza conexiunea oricând ai nevoie, conectându-te automat la locația optimă a serverului.

Pentru a obține trafic nelimitat și acces nerestricționat la conținutul din întreaga lume alegând o locație de server în funcție de preferințe, efectuează upgrade la versiunea Premium.

Poți face oricând upgrade la versiunea Bitdefender Premium VPN apăsând butonul **AActivare Premium VPN** disponibilă în fereastra VPN. Există două tipuri de abonamente disponibile: abonamente anuale și abonamente lunare.

Abonamentul Bitdefender Premium VPN este independent de abonamentul gratuit Bitdefender Mobile Security for iOS, ceea ce înseamnă că îl vei putea folosi pe toată durata de valabilitate. În cazul în care abonamentul Bitdefender Premium VPN expiră, vei reveni automat la planul gratuit.

Bitdefender VPN este un produs pentru mai multe platforme, disponibil în cadrul produselor Bitdefender compatibile cu Windows, macOS, Android și iOS. După ce faci upgrade la planul Premium, îți vei putea folosi abonamentul pe toate produsele, cu condiția să te conectezi cu același cont Bitdefender.

Notă

De asemenea, Bitdefender VPN funcționează și ca o aplicație independentă pe toate sistemele de operare compatibile, și anume pe Windows, macOS, Android și iOS.

6.8. Confidențialitate cont

Funcția Confidențialitate cont Bitdefender detectează dacă s-au produs scurgeri de informații din conturile pe care le folosești pentru a efectua plăți și cumpărături online sau pentru a te conecta la diverse aplicații sau site-uri web. Datele care ar putea fi stocate într-un cont includ parole, date privind cardurile de credit sau informații privind contul bancar și, dacă acestea nu sunt securizate în mod corespunzător, se poate produce un furt de identitate sau o încălcare a confidențialității.

Starea de confidențialitate a unui cont este afișată imediat după validare.

Pentru a verifica dacă un cont a fost accesat neautorizat, selectează opțiunea **Scanează pentru depistarea accesărilor neautorizate**.

Pentru a începe să-ți păstrezi în siguranță datele personale:

1. Apasă pe pictograma din partea de jos a ecranului.
2. Atinge **Adăugare cont**.
3. Introdu adresa ta de e-mail în câmpul corespunzător și apoi selectează **Continuă**.
   Bitdefender trebuie să valideze acest cont înainte de a afișa informații private. Prin urmare, se va trimite un e-mail conținând un cod de validare către adresa de e-mail furnizată.
4. Verifică-ți inbox-ul și apoi introdu codul primit în secțiunea **Confidențialitate cont** a aplicației. Dacă nu găsești e-mail-ul de validare în Inbox, verifică și directorul Spam.
   Se afișează starea de confidențialitate a contului validat.

Dacă se identifică scurgeri de informații pe oricare dintre conturile tale, îți recomandăm să modifici parola acestora cât mai curând posibil. Pentru a crea o parolă puternică și sigură, ia în considerare aceste sfaturi:

- Folosește cel puțin opt caractere.
- Include litere mari și mici.

- Adaugă cel puțin un număr sau simbol, precum #, @, % sau !.

După securizarea unui cont care a fost implicat într-o scurgere de informații, poți confirma modificările marcând căile de acces neautorizat ca fiind **Rezolvat(e)**. Pentru a face acest lucru:

1. Atinge ··· de lângă breșa pe care ai remediat-o.
2. Atinge **Marchează ca rezolvată**.

După ce toate căile de acces neautorizat sunt marcate ca fiind Rezolvate, contul nu va mai apărea ca fiind implicat într-o scurgere de informații, cel puțin până când nu se detectează o nouă scurgere de informații.

6.9. Întrebări frecvente

Cum poate Bitdefender Mobile Security să mă protejeze împotriva virușilor și a amenințărilor cibernetice?

Bitdefender Mobile Security pentru iOS oferă protecție absolută împotriva tuturor atacurilor cibernetice și este conceput special pentru a-ți păstra datele sensibile departe de privirile indiscrete.

Vei obține o multitudine de caracteristici avansate de siguranță și confidențialitate pentru dispozitivele tale iPhone și iPad - plus multe funcții suplimentare, inclusiv VPN și Protecție Internet.

Bitdefender Mobile Security pentru iOS reacționează instantaneu la viruși și malware, fără a compromite performanța sistemului tău.

Ce tipuri de dispozitive și sisteme de operare acoperă Bitdefender Mobile Security pentru iOS?

Bitdefender Mobile Security pentru iOS îți va proteja telefoanele inteligente și tabletele care rulează cu sistem de operare iOS împotriva tuturor atacurilor cibernetice.

De ce am nevoie de Bitdefender Mobile Security pentru iOS pe sistemul de operare Apple OS?

Unele dintre cele mai importante date sunt stocate pe iPhone sau iPad - și trebuie să ai certitudinea că acestea sunt sigure în permanență. Bitdefender Mobile Security pentru iOS oferă o protecție absolută împotriva atacurilor cibernetice și are grijă de siguranța ta online și de informațiile tale personale, fără a interveni în activitățile tale de zi cu zi.

Primesc VPN odată cu abonamentul meu Bitdefender Mobile Security pentru iOS?

Bitdefender Mobile Security for iOS are integrată o versiune standard pentru Bitdefender VPN care include un volum generos de trafic (200 MB / zi, în total 6 GB lunar), gratuit.

7. VPN

7.1. Ce este Bitdefender Password Manager

VPN-ul servește ca un tunel între dispozitivul dvs. și rețeaua la care vă conectați, securizarea conexiunii, criptarea datelor utilizând criptare militară și ascunderea adresei IP oriunde v-ați afla. Traficul dvs. este redirecționat printr-un server separat; astfel încât dispozitivul dumneavoastră nu poate fi identificat de către ISP-ul dumneavoastră, prin multitudinea de alte dispozitive care utilizează serviciile noastre. În plus, în timp ce sunteți conectat la internet prin Bitdefender VPN, puteți accesa conținut care este în mod normal restricționat în anumite zone.

Notă

Unele țări practică cenzura online, prin urmare utilizarea aplicațiilor VPN pe teritoriul lor este interzisă prin lege. Pentru a evita consecințele legale, este posibil să apară un mesaj de avertizare atunci când încerci să utilizezi caracteristica Bitdefender Password Manager pentru prima dată. Prin continuarea utilizării acestei caracteristici, confirmi că îți sunt cunoscute reglementările aplicabile din țara respectivă și riscurile la care ai putea fi expus.

7.1.1. Protocoale de criptare

Seturile implicite de suite de cifruri activate în clientul și serverul Hydra sunt disponibile mai jos. Toate celelalte suite de cifruri sunt dezactivate.

Suite de cifruri în clientul Hydra:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Notă

Setul pe partea de server este mult mai restrictiv și atât clientul, cât și serverul Hydra vor respinge orice alt mod de criptare în afară de GCM cu algoritm AES. Serverul Hydra susține prioritatea suitelor de cifruri pe partea de server și va respinge handshake-ul TLS dacă este solicitată de client o suită de cifruri mai slabă. Această listă poate fi configurată și în modul Runtime pe partea de server.

7.2. Instalare

7.2.1. Pregătirea pentru instalare

Pentru a instala Bitdefender Password Manager fără probleme, trebuie sa parcurgi acești pași prealabili:

- Asigurați-vă dacă dispozitivul pe care doriți să instalați Bitdefender îndeplinește cerințele de sistem. În cazul în care dispozitivul nu întrunește toate cerințele de sistem, Bitdefender nu va fi instalat sau nu va funcționa în mod corespunzător, determinând reducerea vitezei de funcționare și instabilitatea sistemului.
  Pentru lista completă a cerințelor de sistem, consultă Cerințe de sistem (pagina 235)
- Autentifica-te pe dispozitiv cu datele unui cont de administrator.
- Se recomandă ca, în timpul instalării, dispozitivul tău să fie conectat la internet, chiar atunci când instalarea se face 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.

7.2.2. Cerințe de sistem

- **Pentru utilizatorii de Windows**
  - **Sistem de operare:** Windows 7 cu Service Pack 1, Windows 8, Windows 8.1 Windows 10 și Windows 11
  - **Memorie (RAM):** 1 GB
  - **Spațiu liber disponibil pe hard disk:** 500 MB
  - **Net Framework:** minimum versiunea 4.5.2

> **Important**
> Performanța sistemului poate fi afectată pe dispozitivele care au procesoare de generație veche.

- **Pentru utilizatorii de macOS**
  - **Sistem de operare:** macOS Sierra (10.12) sau o versiune ulterioară
  - **Spațiu liber disponibil pe hard disk:** 100 MB
- **Pentru utilizatorii de Android**
  - **Sistem de operare:** Android 5.0 sau o versiune ulterioară
  - **Spațiu de stocare:** 100 MB
  - O conexiune activă la Internet
- **Pentru utilizatorii iOS**
  - **Sistem de operare:** iOS 12 sau mai recent
  - **Spațiu de stocare pe iPhone:** 50 MB
  - **Spațiu de stocare pe iPad:** 100 MB
  - O conexiune la Internet activă

7.2.3. Instalarea Bitdefender Password Manager

Pentru a începe instalarea, urmează instrucțiunile care corespund sistemului de operare pe care îl utilizezi:

- **Pentru utilizatorii de Windows**
  1. Pentru a începe instalarea Bitdefender Password Manager pe un PC Windows, trebuie doar să descarci kitul de instalare accesând https://www.bitdefender.com/solutions/vpn/download sau e-mailul primit după o achiziție.
  2. Fă dublu clic pe asistentul de instalare pentru a-l executa.
  3. Alege Da dacă se afișează fereastra de dialog UAC (User Account Control).
  4. Așteaptă până la finalizarea descărcării.
  5. Selectează limba produsului, utilizând meniul derulant al instrumentului de instalare.

6. Bifează caseta „Confirm că am citit și sunt de acord cu Contractul de abonament și Politica de confidențialitate”, apoi selectează **LANSARE INSTALARE**.
7. Așteaptă până când instalarea este finalizată.
8. **CONECTEAZĂ-TE** cu contul tău Bitdefender Central. Dacă nu ai un cont Central, înscrie-te pentru a-ți crea unul, selectând butonul **CREARE CONT**.
9. Alege **Am un cod de activare** dacă ai achiziționat un abonament Premium VPN.
   În caz contrar, poți alege **ÎNCEPE VERSIUNEA DE EVALUARE** pentru a testa produsul gratuit timp de 7 zile înainte de a-l achiziționa.
10. Introdu codul pe care l-ai primit prin e-mail, apoi selectează butonul **ACTIVARE PREMIUM**.
11. După o scurtă așteptare, Bitdefender Password Manager este instalat și gata să fie utilizat pe computerul tău.

❍ **Pentru utilizatorii de macOS**

1. Pentru a începe instalarea Bitdefender Password Manager pe un macOS, trebuie doar să descarci kitul de instalare accesând https://www.bitdefender.com/solutions/vpn/download sau e-mailul primit după o achiziție.
2. Instrumentul de instalare va fi salvat pe Mac. În directorul Descărcări, faceți dublu clic pe directorul care conține pachetul .
3. Urmează instrucțiunile de pe ecran. Alege **Continuare**.
4. Va trebui să urmezi pașii de pe ecran necesari pentru a instala Bitdefender Password Manager pe dispozitivul tău Mac. Fă dublu clic pe butonul **Continuare**.
5. Selectează **Confirm**, după ce ai citit și ai confirmat termenii și condițiile contractului de licențiere pentru software.
6. Fă clic pe **Instalare**.
7. Introdu un nume de utilizator și o parolă, apoi selectează **Instalare software**.

8. Vei fi anunțat că a fost blocată o extensie de sistem semnată de Bitdefender. Selectează **Deschide preferințele de securitate**.
9. Selectează pictograma de blocare pentru a debloca extensia. Introdu un nume de utilizator și o parolă, apoi apasă pe **Deblocare**.
10. Selectează **Permite** pentru a încărca extensia de sistem BitdefenderBitdefender. Apoi închide fereastra Securitate și confidențialitate și asistentul de instalare.
11. Accesează pictograma care înfățișează un scut din bara de meniu, apoi **Conectează-te** cu contul tău Bitdefender Central. Dacă nu ai un cont Central, înregistrează-te pentru unul.
12. Alege Am un **cod de activare** dacă ai achiziționat un abonament Premium VPN.
    În caz contrar, poți alege **ÎNCEPE ÎNCERCAREA** pentru a testa produsul gratuit timp de 7 zile înainte de a vă angaja să plătiți pentru el.
13. Introduceți codul primit prin e-mail, apoi faceți clic pe **Activați codul** buton.
14. După o scurtă așteptare, Bitdefender Password Manager este instalat și gata să fie utilizat pe dispozitivul tău Mac.

❍ **Pentru utilizatorii de Android**

1. Pentru a instala Bitdefender Password Manager pe Android, mai întâi deschide aplicația **Google Play Store** pe smartphone-ul sau tableta ta.
2. Caută Bitdefender Password Manager și selectează această aplicație.
3. Apasă pe butonul **Instalare** și așteaptă până la finalizarea descărcării.
4. Apasă **Deschide** pentru a lansa aplicația.
5. Bifează caseta „Sunt de acord cu Contractul de abonament și Politica de confidențialitate”, apoi selectează **Continuare**.
6. **Conectează-te** cu contul tău Bitdefender Central. Dacă nu ai un cont Central, înregistrează-te pentru a-ți crea unul, atingând **Creare cont**.

7. Alege **Am un cod de activare** dacă ai achiziționat un abonament Premium VPN.
   În caz contrar, poți alege Începe versiunea de evaluare de 7 zile pentru a testa produsul gratuit timp de 7 zile înainte de a-l achiziționa.
8. Introdu codul pe care l-ai primit prin e-mail, apoi apasă pe **Activare cod**.

- **Pentru utilizatorii iOS**

1. Pentru a instala Bitdefender Password Manager pe iOS, întâi deschide **App Store** pe iPhone-ul sau iPad-ul tău.
2. Caută Bitdefender Password Manager și selectați această aplicație.
3. Apasă pe pictograma **Obține** și așteaptă până la finalizarea descărcării.
4. Atingeți **Deschis** pentru a rula aplicația.
5. Bifează caseta **Sunt de acord cu Contractul de abonament și Politica de confidențialitate**, apoi selectează **Continuare**.
6. **Conectează-te** cu contul tău Bitdefender Central. Dacă nu ai un cont, înregistrează-te pentru a-ți crea unul, atingând **Creare cont**.
7. Atinge **Permite** dacă dorești să primești notificări Bitdefender Password Manager.
8. Alege **Am un cod de activare** dacă ați achiziționat un abonament Premium VPN.
   În caz contrar, puteți alege Start 7 days Trial pentru a testa produsul gratuit timp de 7 zile înainte de a vă angaja să plătiți pentru el.
9. Introdu codul primit prin e-mail, apoi atinge **Activați codul**.

7.3. Cum să utilizezi Bitdefender VPN

7.3.1. Activare Bitdefender VPN

- **Pentru Windows**
  Pentru a accesa **interfața principală a Bitdefender VPN**, folosește una dintre următoarele metode:

- **Din bara de sistem**
  Fă clic dreapta pe pictograma scut roșu din bara de sistem și apoi selectează opțiunea **Afișare** din meniu.
- **Din interfața Bitdefender**
  Dacă un produs de securitate Bitdefender, precum Bitdefender Total Security sau Bitdefender Antivirus Plus etc., este deja instalat pe computerul tău Windows, poți deschide Bitdefender VPN de acolo:
  1. Fă clic pe **Confidențialitate** din bara din partea stângă a interfeței Bitdefender.
  2. Fă clic pe **Deschide VPN** din panoul VPN.
- **De pe desktop**
  Fă dublu clic pe comanda rapidă Bitdefender VPN de pe desktopul tău.

- **Pentru macOS**

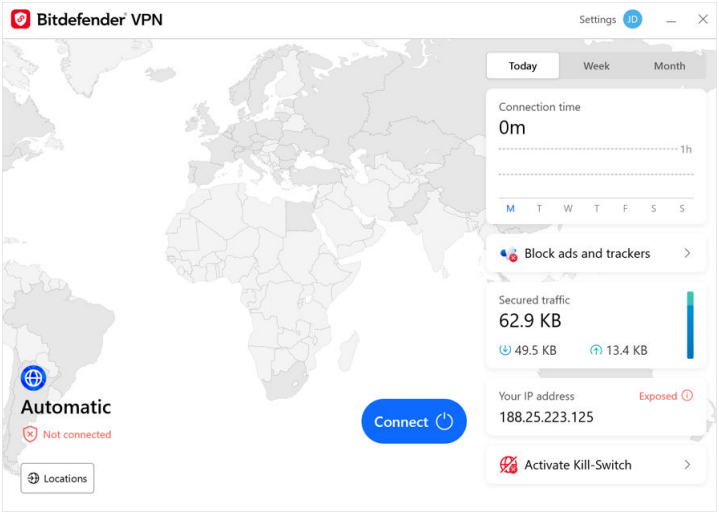
  Poți deschide aplicația Bitdefender VPN făcând clic pe pictograma din bara de meniu din partea dreaptă sus a ecranului.
  Dacă scutul Bitdefender nu apare în bara de meniu, folosește-ți Launchpad-ul Mac sau opțiunea Finder pentru a-l găsi:
  - **Din Launchpad**
    1. Apasă pe **F4** de pe tastatura ta pentru a lansa aplicația Lanchpad pe Mac-ul tău.
    2. Navighează pe paginile cu aplicații instalate până când găsești aplicația Bitdefender VPN. Ca alternativă, poți tasta **Bitdefender VPN** în Launchpad pentru a-ți filtra rezultatele.
    3. Când ai găsit aplicația Bitdefender VPN, fă clic pe pictograma sa pentru a o fixa în bara de meniu.
  - **Din Finder**
    1. Fă clic pe **Finder** în partea de jos stânga a Dock (Finder este pictograma care arată ca un pătrat albastru cu o față zâmbitoare).
    2. Apoi fă clic pe **Go** (Mergi la) în partea stângă sus a ecranului, în bara de meniu.

3. Selectează opțiunea **Aplicații** din meniu pentru a accesa directorul Aplicații de pe Mac-ul tău.
4. Din directorul Aplicații, deschide directorul **Bitdefender** și apoi fă dublu clic pe aplicația **Bitdefender VPN**.

> **Notă**
> Pentru a accesa Bitdefender VPN pe dispozitivele mobile Android sau iOS, trebuie doar să deschizi aplicația Bitdefender VPN după ce ai instalat-o.

7.3.2. Cum să te conectezi la Bitdefender Password Manager

Interfața VPN afișează starea aplicației: activată sau dezactivată. Locația serverului pentru utilizatorii care folosesc versiunea gratuită este setată automat de Bitdefender pe cel mai potrivit server, în vreme ce utilizatorii versiunii premium au posibilitatea de a modifica locația serverului la care doresc să se conecteze selectând-o din lista de Locații virtuale. Pentru a te conecta sau deconecta, trebuie doar să faci clic pe butonul pornire/oprire din interfața VPN.



- **Pentru Windows:** Pictograma barei de sistem afișează o bifă verde atunci când aplicația VPN este activată și o bifă neagră când aceasta

este dezactivată. Atunci când ești conectat la o locație selectată manual, în interfața principală se afișează adresa IP.

- **Pentru macOS:** Pictograma barei de meniu este afișată în culoarea neagră când VPN este activată și în alb când VPN este deconectată. Fă clic pe butonul circular din centrul interfeței și așteaptă stabilirea conexiunii.
- **Pentru Android și iOS:** Pentru a te conecta la Bitdefender VPN pentru Android, iOS și iPadOS:
  - **Din aplicația Bitdefender VPN:** Pentru a activa sau dezactiva aplicația, trebuie doar să atingi butonul pornire/oprire din interfața VPN. Se afișează starea aplicației Bitdefender VPN.
  - **Din aplicația Bitdefender Mobile Security:**
    1. Accesează pictograma VPN din bara de navigare de jos a Bitdefender Mobile Security.
    2. Atinge **ACTIVARE** de fiecare dată când vrei să fii protejat atunci când ești conectat la rețele wireless nesigure. Atinge **DEZACTIVARE** când vrei să dezactivezi conexiunea VPN.

7.3.3. Cum te conectezi la un alt server

Cu un abonament Premium, Bitdefender Password Manager îți permite să te conectezi la oricare dintre serverele noastre din întreaga lume, în orice moment. Pentru a face asta, va trebui să:

1. Deschide aplicația Bitdefender Password Manager
2. Apeși pe butonul **Locație virtuală** în partea interioară a interfeței.
3. Selectezi orice țară dorești.
4. Apeși pe butonul **Conectare la [țara dorită]** în partea interioară a interfeței.

- Pictograma barei de sistem afișează o bifă verde când VPN-ul este conectat.
- Adresa IP a serverului virtual este afișată pe ecranul de pornire în timp ce este conectat la Bitdefender VPN.

- Un rezumat al timpului de conectare, volumul de trafic securizat și ultimele 5 locații la care v-ați conectat sunt afișate și pe tabloul de bord principal.

7.4. Bitdefender Password Manager Setări și caracteristici

7.4.1. Cum să accesezi Setările

Pentru a accesa setările Bitdefender Password Manager, va trebui să urmezi pașii de mai jos:

- **Pe Windows**

  1. Deschide aplicația Bitdefender Password Manager de pe dispozitivul tău, făcând dublu clic pe pictograma acesteia în system tray sau făcând clic dreapta pe aceasta și selectând Afișare.
  2. Selectează butonul **Setări** (reprezentat printr-o rotiță) în partea stângă a interfeței.

- **Pe macOS**

  1. Deschide aplicația Bitdefender Password Manager pe dispozitivul tău macOS selectând pictograma sa din bara de meniu.
  2. Selectează butonul în formă de rotiță din colțul din dreapta sus a interfeței Bitdefender Password Manager și selectează Setări.

- **Pe Android**

  1. Deschide aplicația Bitdefender Password Manager pe dispozitivul tău.
  2. Selectează butonul în formă de rotiță din colțul din dreapta sus a interfeței Bitdefender Password Manager.

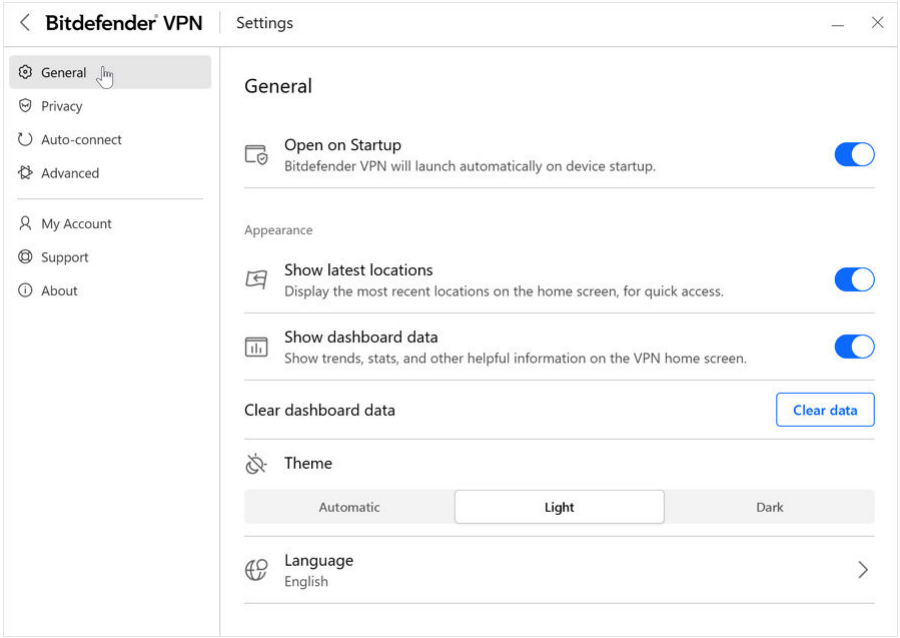
- **Pe iOS**

  1. Deschide Bitdefender Password Manager aplicația pe dispozitivul dvs.
  2. Faceți clic pe butonul roții dințate din colțul din dreapta sus al Bitdefender Password Manager interfata.

7.4.2. General

Aici puteți modifica următoarele:

- **Deschide la pornire**– Bitdefender VPN se va lansa automat la pornirea dispozitivului.
- **Afișează cele mai recente locații**– Afișați cele mai recente locații pe ecranul de start, pentru acces rapid.
- **Afișați datele tabloului de bord** – Afișați tendințe, statistici și alte informații utile pe ecranul de pornire VPN.
- **Ștergeți datele tabloului de bord**– Toate datele din tabloul de bord vor fi șterse și toate contoarele resetate.
- **Temă**– Temă luminoasă/întunecată
- **Limba**– Schimbați limba Bitdefender VPN.
- **Notificări**– Gestionați-vă preferințele de notificări.
- **Ajutați la îmbunătățirea Bitdefender VPN**– Trimiteți rapoarte anonime despre produse pentru a ne ajuta să vă îmbunătățim experiența.
- **Resetează toate setările**– Resetați VPN-ul la setările sale originale fără a-l reinstala.



7.4.3. Caracteristici

Confidențialitate

Internet Kill-Switch

Comutatorul pentru oprirea conexiunii la internet este o nouă funcție care a fost implementată în Bitdefender Password Manager. Atunci când este activat, suspendă temporar tot traficul pe internet în cazul în care conexiunea VPN se întrerupe accidental. Imediat ce revii în mediul online, conexiunea VPN va fi restabilită.

Pentru a activa comutatorul pentru oprirea conexiunii la internet, urmează pașii de mai jos:

- **Pe Windows**

1. Deschide aplicația Bitdefender Password Manager de pe dispozitivul tău, făcând dublu clic pe pictograma acesteia în system tray sau făcând clic dreapta pe aceasta și selectând **Afișare**.

2. Faceți clic pe **Setări** butonul (reprezentat printr-o roată dințată) din partea stângă a interfeței.
3. Selectează opțiunea **Avansat**.
4. Activează opțiunea **Comutator pentru oprirea conexiunii la internet**.

- **Pe Android**
  1. Deschide Bitdefender Password Manager aplicația pe dispozitivul dvs.
  2. Faceți clic pe butonul roții dințate din colțul din dreapta sus al Bitdefender Password Manager interfata.
  3. Din secțiunea **Setări**, activează opțiunea de oprire a conexiunii **Kill-Switch**.

- **Pe iOS**
  1. Deschide Bitdefender Password Manager aplicația pe dispozitivul dvs.
  2. Faceți clic pe butonul roții dințate din colțul din dreapta sus al Bitdefender Password Manager interfata.
  3. Sub **Setări**, activați **Kill-Switch** opțiune.

> **Notă**
> Această caracteristică este disponibilă și pentru dispozitivele macOS cu sisteme de operare 10.15.4 sau versiuni ulterioare.

Ad blocker și Anti-tracker

Aceste caracteristici sunt proiectate să te ajute să îți păstrezi confidențialitatea în siguranță și să te bucuri de lumea digitală fără reclame enervante sau companii care stau cu ochii pe tine. Acestea contribuie la blocarea reclamelor și a programelor de monitorizare online.

Ad blocker

Caracteristica **Ad blocker** este folosită pentru a bloca reclame, ferestre pop-up, reclame video enervante sau bannere publicitare, în timpul navigării. Datorită acesteia, site-urile web se vor încărca mai repede și vor fi mai aerisite, și vei putea interacționa cu ele în siguranță.

Pentru a activa Ad blocker:

1. Găsește caracteristica **Ad blocker și Antitracker** în secțiunea **Setări**.
2. Comută butonul în poziția **Pornit**.

Anti-tracker

Funcția **Anti-tracker** se folosește pentru a bloca programele de monitorizare configurate de agențiile de publicitate să te urmărească și să îți alcătuiască un profil online. Unele site-uri web pot funcționa defectuos atunci când se blochează aceste programe, dar adăugarea adreselor URL ale site-urilor respective pe lista albă poate remedia această problemă.

Pentru a activa Anti-tracker:

1. Localizați **Blocant reclame și Antitracker** caracteristică în **Setări**.
2. Comutați comutatorul la **PE** poziție.

Lista de excepții

Este posibil ca unele site-uri web să nu se încarce corespunzător în cazul în care codul tracker și reclamele acestora sunt blocate. Adăugarea adreselor URL ale acestor domenii pe lista albă poate remedia problema, dar reține că, în timp ce navighezi pe aceste site-uri web, vei vedea reclame și codul lor tracker va fi activ.

Adaugă site-uri web cărora vrei să le permiți să afișeze reclame și să utilizeze trackere astfel:

1. Localizați **Blocant reclame și Antitracker** caracteristică în **Setări**.
2. Fă clic pe linkul **Gestionare**. Apoi, accesează secțiunea Listă albă din această fereastră și apasă pe linkul **Gestionare** corespunzător.
3. Fă clic pe **Adăugare site web** și introdu adresa URL dorită.

Conectare automată

Atunci când te deplasezi, lucrezi dintr-o cafenea sau aștepți în aeroport, conectarea la o rețea wireless publică pentru a face plăți, verifica e-mail-ul sau conturile pe rețelele sociale poate fi soluția cea mai rapidă. Însă pot exista curioși care să încerce să-ți fure datele personale, urmărind informațiile care trec prin rețea.

Pentru a te proteja împotriva pericolelor la care te expun hotspot-urile wireless publice nesecurizate și necriptate, Bitdefender Password

Manager include o funcție de auto-conectare. Asta înseamnă că Bitdefender Password Manager poate fi activat automat în anumite situații, în funcție de preferințele tale și de sistemul de operare pe care îl rulezi.

- În **Windows**, caracteristica de auto-conectare poate fi activată pentru următoarele situații:
  - **Pornire:** Activează VPN de la pornirea Windows.
  - **Rețea Wi-Fi nesecurizată:** Utilizează VPN atunci când te conectezi la rețelele Wi-Fi publice sau nesecurizate.
  - **Aplicații peer-to-peer:** Activează VPN atunci când lansezi o aplicație de partajare a fișierelor de tip peer-to-peer.
  - **Aplicații și domenii:** Folosește întotdeauna VPN când accesezi anumite aplicații și site-uri web.

    Notă

    1. Fă clic pe linkul **GESTIONARE**.
    2. Navighează la locația aplicației pentru care dorești să utilizezi VPN-ul, selectează denumirea aplicației și fă clic pe **Adăugare**.

  - **Categorii de site-uri web:** Activează VPN atunci când accesezi anumite categorii de site-uri web. Bitdefender VPN se poate activa automat pentru următoarele categorii de site-uri web:
    - Financiar
    - Plăți online
    - Sănătate
    - Partajare de fișiere
    - Întâlniri online
    - Conținut pentru adulți

    Notă

    Pentru fiecare categorie, poți selecta un server diferit la care să se conecteze aplicația VPN.

- În **macOS**, caracteristica de auto-conectare poate fi activată pentru următoarele situații:
  - **Pornire:** Activează VPN de la pornirea macOS.
  - **Wi-Fi nesecurizat:** Utilizați VPN-ul ori de câte ori vă conectați la rețele Wi-Fi publice sau nesecurizate.
  - **Aplicații peer-to-peer:** Conectați-vă la VPN când porniți o aplicație de partajare de fișiere peer-to-peer.
  - **Aplicații:** Activează întotdeauna VPN pentru anumite aplicații.
- Pe **Android** și **iOS** Bitdefender Password Manager poate fi configurat pentru a se activa automat doar atunci când folosești rețele Wi-Fi nesecurizate sau publice.

Avansat

Split tunneling (Tunel distinct)

Caracteristica de tunel divizat (split tunneling) a rețelei private virtuale (VPN) îți permite să direcționezi o parte din traficul aplicațiilor sau dispozitivelor printr-un VPN criptat, în timp ce alte aplicații sau dispozitiv au acces direct la internet. Această caracteristică este, în mod special, utilă dacă dorești să beneficiezi de servicii care funcționează cel mai bine atunci când locația ta este cunoscută, bucurându-te în același timp de acces sigur la comunicări și date care pot fi sensibile.

Prin activarea caracteristicii **Split tunneling** (tunel divizat), anumite aplicații și site-uri web vor evita canalul VPN și vor accesa direct internetul.

Pentru a gestiona aplicațiile și site-urile web care evită canalul VPN:

1. Fă clic pe linkul de **Gestionare** după ce ai activat caracteristica.
2. Fă clic pe butonul **Adăugare**.
3. Navighează la locația aplicației în cauză sau introdu URL-ul site-ului web dorit, apoi fă clic pe **Adăugare**.

> **Notă**
> Prin adăugarea unui site web, întregul domeniu, inclusiv toate subdomeniile acestuia, vor fi evitate.

> **Important**
> Pe dispozitivele **macOS**, caracteristica de tunel divizat (Split tunneling) este disponibilă doar pentru site-uri web.

Optimizarea traficului aplicațiilor

Caracteristica Optimizarea traficului aplicațiilor a Bitdefender Password Manager îți permite să stabilești traficul cu prioritate pentru aplicațiile cele mai importante pe dispozitivul tău fără să îți expui conexiunea la riscuri pentru confidențialitate. Aplicațiile VPN redirecționează traficul de internet printr-un tunel sigur fără să folosească algoritmi de criptare puternici pentru a-l proteja.

Însă, această combinație de tehnici poate prezenta anumite dezavantaje, care se referă în principal la viteza conexiunii. Anumiți factori pot provoca încetinirea conexiunii, cel mai frecvent fiind distanța față de serverul la care ești conectat, traficul aglomerat pe rețea și utilizarea mare a lățimii de bandă. Dacă ai simțit că uneori Bitdefender Password Manager generează o povară inutilă asupra conexiunii tale și observi constant o încetinire, există o soluție mai bună decât deconectarea.

Cum funcționează caracteristica Optimizarea traficului aplicațiilor?

Anumite aplicații și servicii, precum platformele de streaming, clienții de torente și jocurile necesită o lățime de bandă mai mare. Utilizarea continuă a acestora ți-ar putea afecta viteza conexiunii la internet. Redirecționarea traficului printr-un tunel VPN oricum provoacă o încetinire a conexiunii tale. Suprasolicitarea conexiunii îți poate afecta serios experiența online.

Caracteristica Optimizarea traficului aplicațiilor a Bitdefender Password Manager te poate ajuta să combați problema încetinirii conexiunii VPN, prin asocierea acestei conexiuni cu prioritate cu aplicația dorită. Funcția îți permite să decizi ce aplicații ar trebui să primească mare parte din trafic, apoi alocă resursele în mod corespunzător. De exemplu, dacă ești într-o întâlnire și observi că apelul tău are o calitate sub cea normală, Optimizarea traficului aplicațiilor îți permite să aloci traficul cu prioritate aplicației de conferință video pentru rezultate mai bune.

În mod normal, utilizatorii VPN ar recurge la închiderea tuturor proceselor de pe dispozitiv care interferează cu calitatea conexiunii sau chiar la dezactivarea conexiunii VPN pentru a obține o viteză de internet mai mare. Caracteristica Optimizarea traficului aplicațiilor îți permite să te bucuri de

protecție neîntreruptă a confidențialității tale fără compromiterea vitezei conexiunii.

Utilizarea caracteristicii Optimizarea traficului aplicațiilor

Momentan, această caracteristică este disponibilă doar pe dispozitivele Windows și îți permite să aloci trafic cu prioritate pentru până la 3 aplicații.

Urmează acești pași pentru a o activa și a o configura cu un efort minim:

1. Lansează aplicația Bitdefender VPN pe computerul tău Windows.
2. Fă clic pe butonul din bara laterală pentru a accesa setările conexiunii VPN.
3. Accesează fila **General** și activează caracteristica **Optimizarea traficului aplicațiilor**. Culoarea butonului se va schimba din gri în albastru.

Pentru a gestiona aplicațiile selectate ca prioritare de această caracteristică:

1. Apasă pe**Administra**legătură.
2. Navighează la locația aplicației pentru care dorești să optimizezi traficul, selectează denumirea aplicației, apoi fă clic pe **Adăugare**. Aplicația va apărea la secțiunea **Cu prioritate**.

> **Notă**
> Ca alternativă, dacă ai deschis recent aplicația pe care dorești să o selectezi ca prioritară, apasă butonul + în fereastra Optimizarea traficului aplicațiilor.

3. Dezactivează și reactivează Bitdefender VPN după ce ai adăugat și ai eliminat aplicații din listă.

Pentru a elimina o aplicație din Optimizarea traficului aplicațiilor, trebuie doar să faci clic pe pictograma de lângă denumirea aplicației.

> **Notă**
> Aplicația de optimizare a traficului nu este disponibil pe macOS.

Protocol

Aici puteți alege tipul de protocol pe care doriți să îl utilizați pentru transferul de date. Sunt disponibile următoarele opțiuni:

- **Automat** - Bitdefender VPN va selecta protocolul optim pentru dispozitivul și rețeaua dvs.
- **Catapulta Hidra** - Rapid și sigur, ideal pentru streaming și jocuri.
- **OpenVPN UDP** - Optimizat pentru viteze mari. Cu toate acestea, acest protocol nu este la fel de fiabil în ceea ce privește pierderea de date precum alte protocoale din listă.
- **OpenVPN TCP** - Proiectat pentru fiabilitate. Se asigură că datele dvs. sunt livrate în întregime, dar nu sunt la fel de rapide ca OpenVPN UDP.
- **Apărător de sârmă** - Protocol mai nou, oferind securitate puternică și un nivel ridicat de performanță.

Salt dublu

Cu această caracteristică puteți gestiona serverele prin care să trimiteți și să criptați dublu traficul dvs. de internet. Datele tale vor trece prin două servere VPN în loc de unul, ceea ce face mai dificilă urmărirea activității tale pe internet.

Notă
Puteți adăuga doar un total de 5 locații cu salt dublu. Cu toate acestea, puteți șterge salturile duble personalizate din lista dvs. și puteți crea altele oricând.

Important
Utilizarea serverelor situate pe continente diferite în același salt dublu poate încetini viteza conexiunii.

7.5. Cum să dezinstalezi Bitdefender Password Manager

Procedura de dezinstalare a aplicației Bitdefender Password Manager este similară celei utilizate pentru ștergerea altor programe din computerul tău:

- **Dezinstalarea Bitdefender Password Manager de pe dispozitivele Windows**

- În **Windows 7**:
  1. Fă clic pe **Start**, accesează **Panoul de control** și fă dublu clic pe **Programe și caracteristici**.
  2. Găsește **Bitdefender Password Manager** și selectează **Dezinstalare**.
     Așteaptă până când procesul de dezinstalare este finalizat.
- În **Windows 8** și **Windows 8.1**:
  1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
  2. Fă clic pe **Dezinstalează un program** sau pe **Programe și caracteristici**.
  3. Găsi **Bitdefender Password Manager** și selectați **Dezinstalează**.
     Așteptați finalizarea procesului de dezinstalare.
- În **Windows 10** și **Windows 11**:
  1. Fă clic pe **Start**, apoi pe **Setări**.
  2. Fă clic pe pictograma **Sistem** din secțiunea Setărilor, apoi selectează **Aplicații instalate**.
  3. Găsi **Bitdefender Password Manager** și selectați **Dezinstalează**.
  4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
     Așteptați finalizarea procesului de dezinstalare.

- **Dezinstalarea de pe dispozitivele macOS**
  1. Fă clic pe **Go** (Mergi la) din bara de meniu și selectează **Aplicații**.
  2. Fă dublu clic pe directorul **Bitdefender**.
  3. Execută **BitdefenderUninstaller**.
  4. În noua fereastră, bifează caseta de lângă **Bitdefender Password Manager**, apoi selectează **Dezinstalează**.
  5. Introdu un cont valid de administrator și o parolă, apoi selectează**OK**.

6. În final, vei fi anunțat că Bitdefender Password Manager a fost dezinstalat cu succes. Selectează **Închide**.

- **Dezinstalarea de pe dispozitivele Android**
  1. Deschide aplicația **Play Store**.
  2. Caută **Bitdefender Password Manager**.
  3. De pe pagina magazinului de aplicații Bitdefender Password Manager selectează **Dezinstalare**.
  4. Confirmă atingând **OK**.

- **Dezinstalarea de pe dispozitivele iOS**
  1. Ține degetul pe aplicația Bitdefender Password Manager.
  2. Selectează opțiunea **Ștergere aplicație**.
  3. Atinge **Ștergere**.

7.6. Întrebări frecvente

Când ar trebui să utilizez Bitdefender VPN?

Trebuie să procedezi cu atenție atunci când accesezi, descarci sau încarci conținut pe internet. Pentru a te asigura că rămâi în siguranță în timp ce navighezi pe internet, îți recomandăm să folosești VPN în următoarele situații:

- când dorești să te conectezi la rețele wireless publice
- dorești să accesezi conținut care în mod normal este restricționat în anumite zone, indiferent dacă ești acasă sau în străinătate
- dorești să-ți păstrezi confidențialitatea datelor personale (nume de utilizator, parole, datele cardului de credit etc.)
- când dorești să-ți ascunzi adresa IP

Pot alege un oraș cu Bitdefender VPN?

Da. Momentan, Bitdefender VPN pentru Windows, macOS, Android și iOS poate fi folosit pentru a selecta un anumit oraș. Iată lista orașelor disponibile în prezent:

- **SUA:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Canada:** Montreal, Toronto, Vancouver
- **Regatul Unit:** Londra, Manchester

Aplicația Bitdefender VPN poate fi instalată ca o aplicație autonomă?

Aplicația VPN este instalată automat împreună cu soluția de securitate Bitdefender. De asemenea, poate fi instalată ca aplicație autonomă din pagina produsului, din Google Play Store și App Store.

Va comunica Bitdefender adresa mea IP și datele mele personale unor terți?

Nu, cu Bitdefender VPN confidențialitatea ta este 100% sigură. Nimeni (agenții de publicitate, ISP, companii de asigurări etc.) nu va avea acces la jurnalele tale online.

Ce algoritm de criptare folosește?

Bitdefender VPN folosește protocolul Hydra pe toate platformele, criptare AES pe 256 de biți sau cel mai înalt cifrat disponibil acceptat atât de client, cât și de server, cu Perfect Forward Secrecy. Aceasta înseamnă că cheile de criptare sunt generate pentru fiecare nouă sesiune VPN și șterse din memorie când sesiunea se termină.

Pot avea acces la conținut restricționat geografic?

Cu VPN Premium ai acces la o rețea extinsă de locații virtuale în întreaga lume.

Va avea un impact negativ asupra autonomiei bateriei dispozitivului meu?

Bitdefender VPN este conceput să îți protejeze datele personale, să îți ascundă adresa IP în timp ce ești conectat la rețele wireless nesecurizate și la conținutul cu acces restricționat din anumite țări. Pentru a evita consumarea inutilă a bateriei, îți recomandăm să folosești funcția VPN numai atunci când ai nevoie de ea și să te deconectezi atunci când ești offline.

De ce aplicația VPN îmi încetinește conexiunea la internet?

Bitdefender VPN este concepută pentru a oferi o experiență ușoară în timp ce navighezi pe web. În funcție de distanța dintre locația ta reală și

locația serverului la care alegi să te conectezi, este de așteptat să existe o anumită scădere a vitezei, însă este aproape întotdeauna suficient de mică încât să treacă neobservată în timpul activității normale online. Mai mult, ne bazăm pe una dintre cele mai rapide infrastructuri VPN din lume. Dacă nu este obligatoriu să te conectezi din locația ta la un server găzduit la mare distanță (de exemplu, din SUA până în Franța), îți recomandăm să îi permiți VPN-ului să se conecteze automat la cel mai apropiat server sau să găsească un server mai aproape de locația ta actuală.

8. MANAGER DE PAROLE

8.1. Ce este Bitdefender Password Manager

Bitdefender Password Manager este un serviciu multi-platformă conceput să ajute utilizatorii să stocheze și să-și organizeze toate parolele utilizate în mediul online. Acesta integrează cei mai siguri algoritmi criptografici cunoscuți în prezent, oferind siguranță și securitate digitală la cel mai înalt nivel. Acesta funcționează ca o extensie de browser și ca o soluție tip aplicație mobilă pentru gestionarea identităților și parolelor și a informațiilor bancare, precum și a altor tipuri de informații confidențiale, utilizate pe mai multe dispozitive.

Bitdefender Password Manager poate salva, completa și genera automat parole și poate gestiona parolele tale pentru toate site-urile web și serviciile online cu ajutorul unei parole principale unice, pentru ca identitatea ta digitală, în ansamblul ei, să fie mai simplu de gestionat.

8.1.1. Securitatea și cum funcționează

Software-ul Bitdefender Password Manager este dezvoltat pe baza celor mai recenți algoritmi criptografici, care asigură nivelul cel mai înalt de securitate pe care și-l pot dori utilizatorii, precum protocoalele AES-256-CCM, SH512, BCRYPT, HTTPS și WSS pentru transmiterea datelor. Toate datele implicate sunt întotdeauna criptate și decriptate pe plan local. Acest lucru garantează faptul că doar posesorul contului poate avea acces la informațiile stocate în cont, precum și la Parola principală utilizată pentru a accesa și utiliza, ulterior, datele respective.

8.2. Introducere

8.2.1. Cerințe de sistem

Poți utiliza cea mai nouă versiune a Bitdefender Password Manager numai pe dispozitivele care rulează următoarele sisteme de operare:

- **Pentru utilizatorii de PC-uri:**
  - Windows 7 cu Service Pack 1
  - Windows 8

- Windows 8.1
- Windows 10
- Windows 11

- **Pentru utilizatorii de macOS:**
  - macOS 10.14 (Mojave) și versiuni ulterioare

> **Notă**
> Reține că performanța sistemului poate fi afectată pe dispozitivele care au procesoare de generație mai veche.

- **Pentru utilizatorii iOS:**
  - iOS 11.0 sau versiuni ulterioare

- **Pentru utilizatorii Android:**
  - Android 5.1 și versiuni ulterioare

> **Notă**
> - Caracteristica de deblocare cu amprenta este disponibilă pe **Android 6.0** și pe versiunile ulterioare.
> - Funcția de completare automată a parolelor este disponibilă pe **Android 8.0** și pe versiuni ulterioare și este compatibilă cu iPhone, iPad și iPod touch.

Cerințe de software

Pentru a putea utiliza Bitdefender Password Manager și toate caracteristicile sale, dispozitivele tale Windows și macOS trebuie să îndeplinească următoarele cerințe de software:

- **Microsoft Edge** (bazat pe Chromium 80 și versiuni ulterioare)
- **Mozilla Firefox** (versiunea 65 sau ulterioară)
- **Google Chrome** (versiunea 72 sau versiuni ulterioare)
- **Safari** (versiunea 12 sau versiuni ulterioare)

> **Notă**
> Cerințele de software nu se aplică sistemelor de operare Android și iOS.

Avertizare

Dacă cerințele de sistem descrise mai sus nu sunt îndeplinite, fie nu vei putea instala Bitdefender Password Manager, fie produsul nu va funcționa corespunzător.

8.2.2. Instalare

Acest capitol îți oferă îndrumări pentru a instala Bitdefender Password Manager pe browserele web atât de pe PC-urile Windows și macOS, cât și de pe dispozitivele mobile Android sau iOS.

Important

Înainte de a-l instala, asigură-te că ai un abonament Password Manager valid în contul tău **Bitdefender Central** pentru ca această extensie de browser să își recupereze validitatea din contul tău.

Abonamentele active sunt enumerate în secțiunea **Abonamentele mele** din contul Bitdefender Central.

Instalarea pe dispozitivele Windows și macOS

Spre deosebire de majoritatea aplicațiilor și programelor care trebuie instalate și configurate pe aceste dispozitive, soluția Password Manager de la Bitdefender este o extensie de browser, care se mai numește și add-on și care poate fi adăugată și activată rapid în browserul tău preferat.

Browserele compatibile cu produsul în prezent sunt: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge** și **Safari**.

1. Accesează https://central.bitdefender.com/ și conectează-te la contul tău.
   Dacă nu ai încă un cont, apasă pe **CREEAZĂ CONT**, apoi introdu numele tău complet, o adresă de e-mail și o parolă.
2. Selectează **Dispozitivele mele** din bara laterală aflată în partea stângă a ecranului.
3. În secțiunea **Dispozitivele mele** apasă pe **+ Adăugare dispozitive**.
4. Această acțiune va genera o fereastră nouă care va apărea pe ecran. În ecranul de selecție, alege **Password Manager**.
5. Alege **Acest dispozitiv**.

Dacă dorești să instalezi produsul pe un alt dispozitiv, selectează Alte dispozitive. Apoi, poți trimite prin e-mail un link de descărcare către dispozitivul respectiv sau poți copia direct URL-ul pentru instalare.

6. Apoi alege browserul pe care dorești să instalezi extensia Password Manager.
7. Fiecare buton corespunzător te va redirecționa la magazinul de extensii al browserului. De acolo trebuie doar să urmezi instrucțiunile de pe ecran, așa cum se arată mai jos:

   Microsoft Edge

   - Apasă pe butonul {1}Obține{2}
   - Apasă pe {1}Adăugare extensie{2} în fereastra care apare pe ecran

   Google Chrome

   - Apasă pe butonul **Adaugă la Chrome**
   - În caseta de confirmare, apasă pe **Adăugare extensie**

   Mozilla Firefox

   - Apasă pe butonul **Adăugare la Firefox**
   - Apasă pe butonul **Instalare** din colțul din dreapta sus al ecranului

   Safari

   - Apasă pe butonul **Obține**, apoi pe **Instalare**
   - Deschide Safari și selectează **Preferințe** din bara de meniu din partea de sus
   - În fereastra Preferințe, apasă pe fila **Extensii**
   - Selectează caseta de bifare de lângă Password Manager pentru a-l activa

După ce ai urmat acești pași, creează o parolă principală puternică, apoi apasă pe butonul **Salvare Parolă principală** după ce ai citit și ți-ai exprimat acordul în legătură cu **Termenii și condițiile**.

> **Important**
> Reține că vei avea nevoie de această Parolă principală pentru a debloca toate parolele, informațiile cardurilor bancare și notițele salvate în Bitdefender Password Manager. În esență, aceasta este cheia care îi permite deținătorului să utilizeze acest produs.

Avertizare

Atunci când creezi Parola principală, vei primi o **cheie de recuperare formată din 24 de cifre**. **Notează cheia de recuperare într-un loc sigur și nu o pierde**. Această cheie este singura cale prin care îți poți accesa parolele salvate în Password Manager în eventualitatea în care **uiți Parola principală** configurată anterior pentru contul tău.

❍ Când ai terminat poți apăsa **Închidere**.

Instalarea pe dispozitivele Android

Cea mai simplă metodă pentru a instala Bitdefender Password Manager pentru telefoanele și tabletele Android, este să descarci aplicația direct din Google Play.

Aplicația Password Manager de la Bitdefender poate fi instalată și din contul **Bitdefender Central**:

1. Pe dispozitivul mobil Android, conectează-te la contul tău Bitdefender Central accesând https://login.bitdefender.com/central/login.
2. Selectați **Dispozitivele mele** în bara laterală din stânga a ecranului.
3. În secțiunea **Dispozitivele mele**, continuați făcând clic pe **+ Adăugați dispozitiv**.
4. Această acțiune va solicita o nouă fereastră să apară. Alege **Password Manager** în ecranul de selecție.
5. Alege **Acest dispozitiv**.
   Dacă dorești să instalezi produsul pe un alt dispozitiv, selectează **Alte dispozitive**. Apoi, poți trimite prin e-mail un link de descărcare către dispozitivul respectiv sau poți copia direct URL-ul pentru instalare.
6. Vei fi redirecționat către **Google Play**. Atinge **Instalare** pentru a descărca Bitdefender Password Manager pe Android.
7. După finalizarea descărcării, deschide aplicația Password Manager.
8. Dacă nu ești conectat automat la contul tău, introdu numele tău de utilizator și parola ta.

După ce ați urmat acești pași, setați o parolă principală puternică, apoi apăsați tasta **Salvați parola principală** butonul după ce ați citit și sunteți de acord cu **Termeni și condiții**.

> **Important**
> Rețineți că veți solicita această parolă principală pentru a debloca toate parolele, informațiile despre cardul de credit și notele salvate în Bitdefender Password Manager. Aceasta este în esență cheia care îi permite proprietarului să utilizeze acest produs.

> **Avertizare**
> La crearea parolei principale, veți primi o **cheie de recuperare din 24 de cifre**. Notați cheia de recuperare într-un loc sigur și nu o pierdeți. Această cheie este singura modalitate de a vă accesa parolele salvate în Managerul de parole în cazul în care vi se întâmplă să **uitați parola principală** configurată anterior pentru contul dvs.

❍ Puteți apăsa **Închide** cand sunteți gata.

9. Creează un **cod PIN format din 4 cifre**, pentru ca atunci când deschizi o altă aplicație și revii la Password Manager să nu trebuiască să-ți introduci din nou parola principală configurată anterior. De asemenea, poți activa autentificarea prin recunoaștere facială sau amprentă, dacă aceste opțiuni sunt disponibile

10. Atinge **Activare completare automată** pentru a configura setările Android de completare automată a parolelor.

> **Notă**
> Dacă omiți acest pas, vei putea activa și personaliza opțiunile Android de completare automată ulterior, urmând instrucțiunile disponibile la Completare automată inteligentă (pagina 272).

11. Ți se va afișa o listă de aplicații care pot completa automat parolele. Alege **Password Manager**; apoi, dispozitivul îți va solicita să confirmi faptul că ai încredere în această aplicație.
Atinge **OK**.

12. Introdu codul PIN pe care l-ai configurat la **pasul 9** pentru a confirma această acțiune.

Instalarea pe dispozitivul tău Android este acum finalizată.

Instalarea pe dispozitivele iOS

Cea mai simplă metodă de instalare a Bitdefender Password Manager pe dispozitivele iOS și iPadOS este de a descărca aplicația din Apple App Store.

Download on the App Store

Instalarea aplicației Bitdefender Password Manager se poate face și prin intermediul dvs Bitdefender Central cont:

1. Pe dispozitivul iPhone sau iPad, conectează-te la contul tău Bitdefender Central accesând https://login.bitdefender.com/central/login.
2. Selectați **Dispozitivele mele** în bara laterală din stânga a ecranului.
3. În **Dispozitivele mele**, continuați făcând clic pe **+ Adăugați dispozitiv**.
4. Această acțiune va solicita o nouă fereastră să apară. Alege **Password Manager** în ecranul de selecție.
5. Alege **Acest dispozitiv**.
   Dacă doriți să instalați pe un alt dispozitiv, selectați **Alte dispozitive**. Apoi puteți trimite prin e-mail un link de descărcare către dispozitivul respectiv sau puteți copia direct adresa URL pentru instalare.
6. Vei fi redirecționat către **App Store**. Apasă pe pictograma cu un nor și o săgeată îndreptată în jos pentru a descărca Bitdefender Password Manager pentru iOS.
7. După ce aplicația a fost instalată, deschide-o și bifează caseta mică de pe ecran. După ce citești și îți exprimi acordul cu **Contractul de abonare**, apasă pe **Continuare**.
8. Dacă nu sunteți conectat automat la contul dvs., conectați-vă folosind numele de utilizator și parola.
   După ce ați urmat acești pași, setați o parolă principală puternică, apoi apăsați tasta **Salvați parola principală** butonul după ce ați citit și sunteți de acord cu **Termeni și condiții**.

Important

Rețineți că veți solicita această parolă principală pentru a debloca toate parolele, informațiile despre cardul de credit și notele salvate în Bitdefender Password Manager. Aceasta este în esență cheia care permite proprietarului să utilizeze acest produs.

Avertizare

La crearea parolei principale, veți primi o **cheie de recuperare din 24 de cifre**. Notați cheia de recuperare într-un loc sigur și nu o pierdeți. Această cheie este singura modalitate de a vă accesa parolele salvate în Managerul de parole în cazul în care vi se întâmplă să **uitați parola principală** configurată anterior pentru contul dvs.

- Puteți apăsa **Închide** cand sunteți gata.

9. Creeaza un **PIN din 4 cifre**, astfel, dacă comutați la o altă aplicație și apoi reveniți la Managerul de parole, nu va trebui să reintroduceți parola principală pe care ați configurat-o anterior. Dacă este disponibil, puteți activa și recunoașterea feței sau autentificarea cu amprentă.

Instalarea pe dispozitivul tău iOS/iPadOS este acum finalizată!

8.2.3. Plan comun

Bitdefender Password Manager Shared Plan permite mai multor utilizatori să acceseze și să utilizeze același abonament. Oferă o abordare centralizată a accesului, administrării și suportului software, oferind o soluție rentabilă pentru partajarea serviciului de gestionare a parolelor între mai mulți utilizatori.

- Persoana responsabilă cu planul de abonament partajat, cunoscut sub numele de Plan Manager, poate partaja serviciul între membri.
- Fiecare membru primește propriul cont unic Bitdefender Central legat de adresa sa de e-mail și acces la serviciul Bitdefender Password Manager.

Partajarea Bitdefender Password Manager cu mai mulți utilizatori

Invitarea membrilor

Pentru a adăuga unul sau mai mulți utilizatori la abonamentul partajat, managerul planului trebuie să urmeze acești pași:

1. Conectați-vă la contul dumneavoastră Bitdefender Central la https://central.bitdefender.com/.
2. Accesați meniul **Abonamentele mele**, situat în partea stângă a paginii.
3. Alegeți opțiunea **Invită un membru** în panoul **Bitdefender Password Manager Shared Plan**.
4. Introduceți adresa de e-mail a fiecărei persoane cu care doriți să partajați abonamentul, apoi faceți clic pe **Trimite**. Se pot adăuga maximum 3 membri deodată.
5. Instrucțiunile de configurare sunt trimise imediat prin e-mail noilor membri. Faceți clic pe butonul **Închide** pentru a ieși din fereastra de confirmare.

> **Notă**
> Membrii au la dispoziție 24 de ore pentru a vă accepta invitația după ce le este trimisă prin e-mail.
>
> - Membrii invitați vor apărea cu statutul „Invitați”.
> - Îi vei vedea ca membri „activi” după ce acceptă invitația. De asemenea, sunteți notificat prin e-mail cu privire la fiecare invitație acceptată.

Eliminarea membrilor

Accesul la Bitdefender Password Manager Shared Plan se pierde pentru membrii care sunt eliminați. Atunci când managerul planului decide să elimine un membru al abonamentului, acesta primește o notificare prin e-mail. Pentru următoarele 30 de zile, fostul membru este trecut la o versiune de evaluare de 30 de zile a Bitdefender Password Manager, cu funcții complete. Apoi, serviciul va fi oprit.

Managerul de plan poate elimina utilizatorii din planul partajat în felul următor:

1. Conectați-vă la contul Bitdefender Central la https://central.bitdefender.com/.
2. Mergeți la meniul **Abonamentele mele**, situat în partea stângă a paginii.
3. În panoul **Bitdefender Password Manager Shared Plan** faceți clic pe **Administrează**, apoi alegeți **Editare membrii** din meniu.

4. Faceți clic pe butonul **Elimină** pentru a scoate un membru din planul partajat.
5. Alegeți **Da, elimină membru**, apoi faceți clic pe butonul **Finalizare editare** pentru ca modificările să intre în vigoare.

> **Notă**
> Atunci când un membru este șters din planul partajat, statutul acestuia apare **În așteptare** până când este eliminat complet.

Acceptarea unei invitații

Veți primi un e-mail când cineva vă invită să deveniți membru cu abonament pentru Planul comun Bitdefender Password Manager. Ai la dispoziție 24 de ore pentru a accepta o invitație după ce ți-a fost trimisă.

Pentru a accepta invitația și pentru a obține acces la funcțiile managerului de parole, utilizatorul trebuie să urmeze acești pași:

1. Deschideți e-mailul pe care l-ați primit cu titlul **[Începe să folosesti abonamentul Bitdefender ca membru]** și faceți clic pe butonul **ACTIVEAZĂ ÎN CENTRAL**.
2. Pagina Bitdefender Central se va deschide apoi în browserul dvs.
   - Dacă aveți deja un cont de utilizator Bitdefender asociat cu e-mailul prin care a fost trimisă invitația, **conectați-vă** pentru a vă revendica abonamentul partajat.
   - Dacă nu aveți un cont de utilizator Bitdefender, faceți clic pe **Creare unul** și înregistrați-vă cu același e-mail cu care a fost trimisă invitația pentru a vă revendica abonamentul partajat.
     - Introduceți numele dvs. complet
     - Introduceți adresa dvs. de e-mail
     - Introduceți parola
     - Faceți clic pe butonul Create Account și veți fi semnat.
3. După ce vă conectați, faceți clic pe **Începe** în ecranul de întâmpinare care vă informează că abonamentul dumneavoastră la Bitdefender Password Manager este acum activ.
4. Urmați pașii de pe ecran descriși și în Instalare (pagina 259).

> **Notă**
> E-mailul managerului de plan este afișat în contul tău Bitdefender Central în partea de sus a meniului Manager parole și pe cardul de abonament, sub Abonamentele mele.
>
> Dacă aveți nevoie de asistență cu planul comun, vă rugăm să luați legătura cu ei.

8.3. Importarea și exportarea parolelor

Bitdefender Password Manager este gândit astfel încât să faciliteze o comunicare și un transfer al datelor eficient către sursele externe, platformele și instrumentele tip software. Acesta este motivul principal pentru care necesitatea des întâlnită de a importa sau exporta parole în și din Bitdefender Password Manager poate fi îndeplinită cu ușurință.

8.3.1. Compatibilitate

Bitdefender Password Manager poate transfera date cu ușurință de la aplicațiile din următoarea listă:

- **1Password**
- **Bitwarden**
- **Bitdefender Password Manager**
- **ByePass**
- **Chrome browser**
- **Claro**
- **Dashlane**
- **Edge browser**
- **ESET Password Manager v2**
- **ESET Password Manager v3**
- **StickyPassword**
- **Watchguard**
- **Firefox browser**
- **Gestor de contraseñas – Claro**

- **Gestor de contraseñas – SIT**
- **Gestor de contraseñas – Telnor**
- **KeePass 2.x**
- **LastPass**
- **Panda Dome Passwords**
- **PassWatch**
- **Saferpass**
- **SFR Cybersécurité**
- **SIT**
- **F-Secure**
- **Telnor**

> **Notă**
> Dacă denumirea browserului sau a instrumentului de gestionare a parolelor de la care încerci să transferi fișiere de date nu apare pe lista furnizată mai sus, poți urma ghidul nostru online care le arată utilizatorilor cum să editeze un fișier CSV provenit de la soluții necompatibile de gestionare a parolelor, pentru a-ți putea importa informațiile în **Bitdefender Password Manager**: https://www.bitdefender.ro/consumer/support/answer/21762/

Acest transfer de date între Bitdefender Password Manager și un alt software de administrare a conturilor poate fi realizat prin următoarele formate de date:

CSV, **JSON**, **XML**, **TXT**, **1pif** și **FSK**.

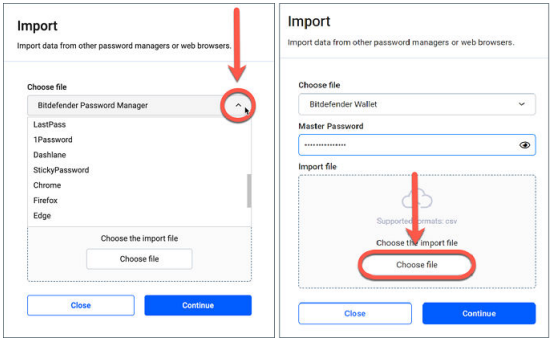
8.3.2. Importarea în Password Manager

Bitdefender Password Manager îți permite să imporți cu ușurință parolele din alte soluții de gestionare a parolelor și browsere. Dacă intenționezi să optezi pentru Bitdefender Password Manager în locul altui serviciu de gestionare a parolelor, probabil ai stocat un volum considerabil de date conectare precum nume de utilizator, parole și alte date de autentificare necesare pentru toate conturile tale.

Acum că ai ales Bitdefender Password Manager, vei dori să imporți acele date salvate în această soluție.

Iată cum poți importa în Bitdefender Password Manager informațiile stocate în alte aplicații și browsere web, **indiferent de sistemul de operare** pe care ai ales să instalezi acest produs:

1. Apasă pe pictograma produsului Password Manager în browserul tău web (pe Windows sau macOS) sau lansează aplicația Password Manager (pe Android sau iOS). Introdu **Parola ta principală**, dacă ți se solicită acest lucru.
2. Deschide meniul Password Manager pentru a extinde bara laterală din partea stângă și apasă pe elementul **Setări** din meniu.
3. Derulează în jos la secțiunea **Date** și apasă pe opțiunea **Importare date**.
4. Utilizează meniul derulant pentru a selecta denumirea aplicației de gestionare a parolelor sau browserul din care dorești să-ți imporți conturile. Introdu **Parola principală** în câmpul corespunzător, apoi apasă pe **Alege fișier**.



5. Răsfoiește directoarele tale pentru a găsi locația în care ai salvat fișierul care conține numele de utilizator și parolele, exportate din cealaltă soluție de gestionare a parolelor sau browser web, apoi apasă pe **Continuare**.

Odată importate, parolele tale vor fi apoi accesibile pe toate dispozitivele unde ai instalat aplicația sau extensia de browser Bitdefender Password Manager.

8.3.3. Exportarea din Password Manager

Dacă vrei vreodată să optezi pentru un alt serviciu de gestionare a parolelor, Bitdefender Password Manager îți permite să exporți cu ușurință parolele salvate (inclusiv date de autentificare în conturi, note securizate etc.) într-un fișier CSV (valori separate prin virgulă) sau într-un fișier criptat, pentru ca despărțirea ta de Bitdefender Password Manager să nu fie un proces dificil.

> **Important**
> Un fișier CSV **nu** este criptat și conține numele de utilizator și parolele în format text simplu, ceea ce înseamnă că informațiile tale confidențiale pot fi citite de oricine are acces la dispozitivul tău. Prin urmare, îți recomandăm să urmezi instrucțiunile de mai jos pe un dispozitiv sigur.

Iată cum îți poți exporta datele din Bitdefender Password Manager:

1. Faceți clic pe pictograma Password Manager din browserul dvs. web (pe Windows sau macOS) sau lansați aplicația Password Manager (pe Android sau iOS). Dacă vi se solicită, introduceți Parola principala.
2. Deschide meniul Password Manager pentru a extinde bara laterală din partea stângă și apasă pe elementul **Setări** din meniu.
3. Derulează în jos la secțiunea **Date** și apasă pe opțiunea **Exportare date**.
4. Acum ar trebui să ai la dispoziție următoarele două opțiuni:
   - **CSV**
   - **Fișiere protejate prin parolă**

   Selectează opțiunea preferată, apoi introdu Parola principală și apasă pe butonul **Exportare date**.

   > **Notă**
   > Dacă ai ales opțiunea fișierului protejat prin parolă, ți se va solicita să criptezi cu o parolă datele care conțin lista conturilor, astfel că numai tu le poți accesa, dacă este cazul.

5. Apoi, browserul web/aplicația va salva un fișier cu denumirea Bitdefender Password Manager_exported_data_current-date în

sistemul tău, în directorul implicit de descărcare. Acest fișier conține toate datele tale stocate în Bitdefender Password Manager.

După exportarea datelor tale, le poți încărca în soluția pe care ai ales-o pentru gestionarea parolelor.

8.4. Caracteristici și funcții

Acest capitol îți va descrie toate caracteristicile și funcțiile Bitdefender Password Manager și îți va explica utilitatea lor și cum să le valorifici la maximum.

8.4.1. Gestionarea parolelor

Generator parolă

Când vine vorba de securitatea online, regula de aur este să utilizezi întotdeauna fraze de acces unice pentru fiecare serviciu care presupune crearea unui cont. Reutilizarea parolelor pe mai multe platforme este cauza principală a furturilor de identitate și pierderilor de date asociate preluării ostile a conturilor.

Această caracteristică îi ajută pe utilizatori să genereze parole sigure, complexe și unice pentru fiecare cont nou pe care îl creează online. Acest lucru elimină nevoia ca utilizatorii să inventeze singuri parole puternice sau să aibă grijă să nu utilizeze aceeași parolă pentru mai multe conturi.

Modulul **Generator de parole** poate fi accesat de la fila din partea de sus a interfeței Password Manager.

Generatorul poate fi setat să creeze parole care să conțină **între 4 și 32 de caractere**.

De asemenea, poți specifica tipul de caractere care ar trebui să apară sau nu în parola generată aleatoriu, prin bifarea sau debifarea casetelor corespunzătoare.**(literă mică, literă mare, cifre, caractere speciale)**

Dacă apeși pe butonul din partea dreaptă a parolei afișate, generatorul va modifica parola specificată.

Pentru a utiliza parola afișată, apasă pe **Utilizare parolă**, ceea ce va salva șirul de caractere în clipboard.

Notă
Parolele tale generate anterior vor fi stocate temporar în istoricul parolelor, care poate fi accesat de la butonul **Istoricul parolelor**.

Colectarea parolelor

Cu această caracteristică a Password Manager, ți se va solicita să stochezi toate parolele tale noi imediat după crearea lor. Password Manager le va solicita utilizatorilor să stocheze parolele nou create, pentru a fi adăugate unui mediu cu un nivel înalt de securitate furnizat de Bitdefender chiar atunci.

Completare automată inteligentă

Bitdefender Password Manager poate fi configurat astfel încât să poată completa automat datele tale de autentificare și cele mai importante parole. Algoritmii brevetați pot detecta și completa automat datele de autentificare pe site-urile web vizitate anterior, economisind timpul utilizatorilor de fiecare dată când se conectează la un serviciu.

1. În Windows sau macOS, apasă pe pictograma **Password Manager** în browserul tău web.

   În Android sau iOS, lansează aplicația **Password Manager**. Introdu **Parola ta principală**, dacă ți se solicită acest lucru.

2. Deschide meniul Password Manager pentru a extinde bara laterală din partea stângă și apasă pe elementul **Setări** din meniu.
3. Apasă pe **Setări dispozitiv**.
4. Aici vei observa un buton care afișează fie opțiunea **Dezactivare completare automată**, fie opțiunea **Activare completare automată**. Această setare controlează funcționarea caracteristicii de completare automată inteligentă.

Raport de securitate

Raportul de securitate este un instrument care va genera rapoarte pe baza unor caracteristici concepute să îți sporească securitatea digitală. Acesta te informează când o parolă necesită atenția ta imediată, determinând nivelul de securitate al acesteia. De asemenea, va detecta parolele duplicat și îți va solicita să le modifici în mod corespunzător, evitând pericolele asociate reciclării acelorași parole pentru mai multe conturi.

Raportul îți va furniza, cu prioritate, informații despre igiena ta generală în ceea ce privește gestionarea parolelor: aceasta se referă la duplicarea parolelor, utilizarea de parole slabe sau de parole sau adrese de e-mail compromise.

Acest lucru se realizează prin compararea listei de coduri hash criptate de pe pagina web a Troy cu datele locale stocate pe dispozitivul tău pentru a vedea dacă există coduri hash corespondente asociate parolelor tale. Dacă sunt identificate coduri corespondente, vei fi notificat și încurajat să îți modifici parolele și alte date de conectare în mod corespunzător.

Pentru a vizualiza **Raportul de securitate**, accesează interfața Password Manager și selectează butonul corespunzător din bara de sus.

Sincronizarea pe alte platforme

Salvarea parolelor o singură dată în Bitdefender Password Manager îți va permite să le stochezi și să le accesezi cu ușurință pe toate dispozitivele Windows, Mac, Android sau iOS din Chrome, Safari, Firefox și Edge sau din interiorul aplicațiilor mobile.

> **Notă**
> De asemenea, Bitdefender integrează și un **mod offline** pentru accesarea parolelor tale, în cazul în care se întâmplă să nu ai acces la internet. Astfel, parolele tale devin accesibile în orice moment și de oriunde te-ai afla.

Ștergerea unei parole

Pentru a șterge parolele salvate, apasă întâi pe pictograma de editare de lângă parola pe care dorești să o elimini, aflată în fila **Conturi**. Derulează în jos, apoi selectează **Ștergere**. Se va afișa o fereastră în care vei fi întrebat dacă dorești să elimini contul; apasă pe **Elimină**.

8.4.2. Gestionarea conturilor

Autentificare

Autentificarea în Bitdefender Password Manager se realizează prin configurarea codului **PIN** în timpul procesului de instalare a produsului. (Reține: caracteristica **Blocare automată** blochează managerul de parole sau te deconectează după o perioadă de lipsă de activitate a browserului sau la închiderea aplicației mobile)

De asemenea, acest lucru poate fi realizat și prin utilizarea datelor biometrice, dacă aceste caracteristici sunt disponibile, precum **deblocare prin amprentă** sau **recunoaștere facială**.

Pentru a **activa sau dezactiva** autentificarea biometrică:

1. Pe Windows sau macOS, faceți clic pe pictograma **Password Manager** din browserul dvs. web.
   Pe Android sau iOS, lansați **Password Manager** aplicarea.
   Dacă vi se solicită, introduceți Parola principala.
2. Deschideți meniul Password Manager pentru a extinde bara laterală din stânga și faceți clic pe **Setări** din meniu.
3. Click pe **Setări dispozitiv**.
4. Aici vei observa un buton care afișează fie opțiunea **Dezactivare biometrice**, fie opțiunea **Activare biometrice**. Această setare controlează caracteristica de autentificare biometrică.

Resetarea Parolei principale

> **Important**
> Caracteristica **Schimbare Paroleiă principală** nu este disponibilă pe dispozitivele mobile. Singura cale prin care îți poți schimba sau recupera parola principală este prin intermediul extensiei de browser Bitdefender Password Manager de pe un dispozitiv Windows PC sau macOS.

Iată cum îți poți schimba **Parola principală** ca o măsură de precauție și cum poți crea una nou în Bitdefender Password Manager:

1. După ce ai instalat extensia de browser, fă clic pe pictograma Password Manager din bara de instrumente a browserului tău.
2. Introdu parola principală actuală pentru a debloca seiful.

> **Important**
> Dacă nu mai știi care e parola principală actuală, apasă pe opțiunea **Am uitat parola** de pe același ecran. Introdu **Cheia de recuperare formată din 24 de cifre** furnizată odată cu configurarea inițială a Bitdefender Password Manager, apoi tastează o parolă principală nouă. **Dacă nu mai știi care este Parola principală** și nici unde ți-ai notat **Cheia de recuperare**, ultima opțiune este să **contactezi un reprezentant Bitdefender care te va ajuta să-ți resetezi contul**. Resetarea contului tău **va șterge toate datele și parolele tale** salvate în Bitdefender Password Manager.

3. Deschideți meniul Password Manager pentru a extinde bara laterală din stânga și faceți clic pe **Setări** articol din meniu.
4. Apasă pe butonul **Contul meu** din secțiunea **Cont**.
5. Se va afișa o fereastră cu informații despre abonamentul tău Password Manager.
   Apasă pe butonul **Schimbare Parola principală**.
6. Vei fi redirecționat către o fereastră nouă unde vei putea alege o parolă principală nouă. Introdu parola ta principală actuală, apoi tastează o parolă principală nouă. Aceasta trebuie să conțină cel puțin 8 caractere, cel puțin o literă mică, o literă mare și o cifră.
7. Apasă pe butonul **Schimbă** când ai terminat.
8. Așteaptă puțin până când Bitdefender resetează parola principală anterioară.
   Nu închide browserul web!
9. Apoi ți se va furniza o **cheie de recuperare de 24 de cifre** nouă. Notează cheia de recuperare într-un loc sigur și **nu o pierde**. Această cheie este singura cale de a-ți accesa parolele salvate în Password Manager, în cazul în care îți uiți parola principală.
   Când ai terminat, apasă **Închide**.
10. Contul tău Bitdefender Password Manager va fi deconectat.
    Pentru a debloca seiful, utilizează noua parolă principală pe care tocmai ai configurat-o.

8.4.3. Alte funcționalități

Gestionarea identităților

Această caracteristică le permite utilizatorilor să stocheze mai multe identități și soluției Password Manager să completeze automat, într-un mod rapid, simplu și sigur, datele relevante în formularele de pe site-uri web înainte de a face o achiziție.

Ca orice alte date stocate în Password Manager, toate informațiile confidențiale cuprinse în aceste identități stocate sunt criptate și disponibile numai pe dispozitivul utilizatorului.

Pentru a adăuga o identitate la Password Manager:

1. Pe Windows sau macOS, faceți clic pe Password Manager din browserul dvs. web.

   Pe Android sau iOS, lansați **Password Manager**.
   Dacă vi se solicită, introduceți Parola principala.

2. Deschide meniul Password Manager pentru a extinde bara laterală din partea stângă și apasă pe elementul **Identități** din meniu.
3. Apasă pe butonul **Adăugare Identitate** din partea de jos.
4. Completează detaliile pe care dorești să le stochezi, apoi apasă pe **Salvare**.

Administrarea cardurilor bancare

Această caracteristică îți permite să salvezi și să completezi datele cardurilor bancare pentru sesiuni mai simple, mai rapide și mai sigure de cumpărături.

Pentru a adăuga un card bancare la Password Manager:

1. Pe Windows sau macOS, faceți clic pe **Password Manager** din browserul dvs. web.

   Pe Android sau iOS, lansați **Password Manager**.
   Dacă vi se solicită, introduceți Parola principala.

2. Deschide meniul Password Manager pentru a extinde bara laterală din partea stângă și apasă pe elementul **Carduri bancare** din meniu.

3. Apăsați pe butonul **Adăugați identitate** din partea de jos.
4. Completați detaliile pe care doriți să le stocați apoi apăsați **Salvați**.

Securizare

Caracteristica Secure Me îți permite să te deconectezi sau să ștergi istoricul de navigare de pe computerul tău, tabletă sau dispozitivul mobil de la distanță.

Pentru a afla unde este această caracteristică și pentru a o activa:

1. Pe Windows sau macOS, faceți clic pe **Password Manager** din browserul dvs. web.

   Pe Android sau iOS, lansați **Password Manager**.
   Dacă vi se solicită, introduceți Parola principala.
2. Deschide meniul Password Manager pentru a extinde bara laterală din partea stângă și apasă pe elementul **Secure Me** din meniu.
3. Apasă pe butonul **Securizare toate sesiunile**.
   Dacă îți dorești să protejezi un anumit dispozitiv, caută-l în lista de dispozitive unde ai instalat Password Manager sau unde l-ai activat într-un anumit browser.

Note

Caracteristica Note securizate acționează exact ca o agendă confidențială în care poți stoca date sensibile, le poți sorta și poți utiliza culori pentru a le vizualiza mai bine. Nu numai că păstrezi informațiile ordonate, dar acestea sunt și în siguranță.

Pentru a localiza și activa această funcție:

1. Pe Windows sau macOS, faceți clic pe **Password Manager** din browserul dvs. web.

   Pe Android sau iOS, lansați **Password Manager**.
   Dacă vi se solicită, introduceți Parola principala.
2. Deschide meniul Password Manager pentru a extinde bara laterală din partea stângă și apasă pe elementul **Note** din meniu.
3. Apasă pe butonul **Adăugare notă**.

După ce ai notat informația pe care dorești să o păstrezi în siguranță, apasă pe **Salvare**.

8.5. Întrebări frecvente

Întrucât există anumite întrebări în legătură cu Bitdefender Password Manager care au tendința să revină, noi avem răspunsurile! De aici puteți afla mai multe detalii despre contul dvs. Bitdefender, cum să importați parolele, despre protocoalele de securitate a datelor și alte subiecte importante pentru clienții noștri.

Întrebări generale despre Bitdefender Password Manager

Cum pot face ca fereastra pop-up Password Manager să nu mai apară în soluția mea de securitate de la Bitdefender?

Notificarea despre Password Manager afișată în luna august 2022 de Bitdefender Total Security, Internet Security și Antivirus Plus poate fi închisă făcând clic pe butonul „x”. Fereastra „Gestionează-ți parolele cu Bitdefender Password Manager” va mai apărea aleatoriu de câteva ori înainte de a dispărea definitiv. Poți opta să nu mai primești acest mesaj promoțional comutând butonul {1}Notificări cu recomandări{2} din secțiunea Setări Bitdefender în poziția de dezactivare.

Ce se întâmplă când Bitdefender Password Manager expiră?

Când abonamentul tău Password Manager expiră și nu mai este activ, ai la dispoziție cel mult 90 de zile pentru a-ți exporta parolele. Parolele tale vor mai fi păstrate pentru încă 30 de zile, ca back-up. În aceste 90 de zile, vei avea acces numai la funcția de exportare datelor. Nu vei mai putea utiliza Password Manager. Caracteristica de completare automată nu va mai funcția și nici nu vei mai putea genera parole.

La finalul perioadei de grație de 90 de zile, ai la dispoziție încă 30 de zile pentru a contacta serviciul de asistență al Bitdefender și a solicita restituirea parolelor tale în baza de date live. În acel moment, îți vei putea exporta parolele de la Bitdefender Password Manager.

Datele tale vor fi păstrate în baza de date live doar până la finalul zilei în care a fost restabilită la cerere. La miezul nopții, baza de date va fi ștearsă și, dacă nu ai depășit perioada suplimentară de 30 de zile, parolele tale vor putea fi restabilite din nou din datele back-up. Datele neprelucrate din baza de date, păstrate ca back-up, pot fi furnizate la cerere utilizatorului, însă baza de date este criptată și informațiile nu pot fi accesate.

Ce este o Parolă principală și de ce trebuie să o țin minte?

Parola principală este cheia care deblochează accesul la toate parolele stocate în contul tău Bitdefender Password Manager. Parola principală trebuie să conțină cel puțin 8 caractere. De aceea, îți recomandăm să creezi o parolă principală puternică, să o memorezi și să nu o împărtășești nimănui. Pentru a crea o parolă principală puternică, îți recomandăm să utilizezi o combinație de litere mari și litere mici, cifre și caractere speciale (precum #, $ sau @).

Cum pot dezactiva mesajul prin care Bitdefender îmi solicită Parola principală de fiecare dată când deschid browserul?

Atunci când îți blochezi dispozitivul fără să închizi browserul, soluția Password Manager nu se blochează și îți poți accesa datele când revii. Ca o măsură de siguranță, va trebui să te conectezi la contul Bitdefender Central de fiecare dată când deschizi browserul și apoi să introduci Parola principală.

- Pentru a dezactiva mesajul de conectare în contul Central, accesează Setările și bifează opțiunea „Dezactivare mesaj conectare la pornire”.
- Pentru a dezactiva notificarea privind parola principală, bifează caseta „Reține parola” din ecranul Deblochează-ți seiful.

De ce nu stocați Parola principală și ce se întâmplă dacă o uit?

Motivul pentru care nu stocăm Parola ta principală pe serverele noastre este ca tu să fii singurul care are acces la contul tău. Astfel este siguranță. Dacă Bitdefender Password Manager nu-ți recunoaște parola principală, asigură-te că ai introdus-o corect și că tasta Caps Lock nu este activă pe tastatura ta.

Dacă nu mai știi care este parola ta principală, poți utiliza întotdeauna Cheia de recuperare pentru a-ți debloca contul Password Manager. În timpul procesului de conectare, Bitdefender Password Manager generează o {1}cheie de recuperare{2} care poate fi utilizată pentru a redobândi accesul la cont fără a-ți pierde datele.

Dacă nu mai știi care este parola ta și unde ai notat Cheia de recuperare, ca ultimă variantă, contactează un reprezentant Bitdefender pentru a-ți reseta contul.

Important

Resetarea contului tău va șterge toate datele și parolele tale salvate în Bitdefender Password Manager.

Este posibil ca mai mulți utilizatori să folosească un singur abonament Bitdefender Password Manager?

Pentru moment, opțiunea ca mai mulți utilizatori să folosească același abonament Password Manager nu este disponibilă, însă depunem eforturi pentru a face posibilă această caracteristică în curând.

Ce este modul Offline și cum funcționează acesta?

Modul Offline este activat automat în momentul în care conexiunea la internet se pierde în timp ce utilizezi Bitdefender Password Manager. Dacă te-ai conectat deja și ai introdus parola principală, modul Offline îți permite să-ți accesezi parolele când conexiunea la internet nu este disponibilă.

Cum dezinstalez Bitdefender Password Manager?

Pentru a dezinstala Bitdefender Password Manager:

- Pe Windows și macOS:
  Elimină extensia Password Manager din browserul tău web. Fă clic dreapta pe pictograma Bitdefender și selectează „Elimină”.
- Pe Android:
  Apasă lung pe aplicația Password Manager, apoi gliseaz-o în partea de sus a ecranului unde apare mesajul „Dezinstalare”.
- Pe iOS și iPadOS:
  Apasă lung pe aplicația Password Manager până când toate aplicațiile de pe ecran se mișcă, apoi apasă pe X din partea stângă sus a pictogramei Bitdefender.

Întrebări privind confidențialitatea și securitatea Bitdefender Password Manager

Este posibil ca angajații Bitdefender să aibă acces la parolele mele?

Categoric nu. Confidențialitatea ta este prioritatea noastră principală. Acesta este motivul pentru care nu stocăm parola principală pe serverele noastre de date: pentru ca nimeni să nu aibă acces la contul tău, nici măcar angajații companiei. Fiecare parolă și cont sunt criptate la nivel înalt cu cel mai puternic algoritm de securitate a datelor, iar codul pe care îl vedem arată ca un șir aleatoriu de numere și litere amestecate.

Ce s-ar întâmpla dacă serverele Password Manager ar fi compromise?

Fiecare parolă este criptată la nivel local, pe dispozitivul tău, înainte să ajungă la serverele noastre, astfel că dacă hackerii ar încerca să pătrundă în sistemul nostru, ar obține doar pagini de litere și cifre aleatorii fără cheia care le poate decripta. Acest lucru înseamnă că atât tu, cât și datele contului tău sunt întotdeauna păstrate în siguranță de noi.

9. PROTECȚIA IDENTITĂȚII DIGITALE

9.1. Ce este Bitdefender Digital Identity Protection

Confidențialitatea și securitatea online sunt unele dintre principalele puncte de interes pentru utilizatorii de internet din zilele noastre. Și există câteva motive foarte bune pentru asta. Având în vedere că încălcările majore ale datelor au loc de cele mai multe ori, este imperativ să vă asigurați că informațiile dvs. de identificare personală (PII) sunt sigure și securizate.

Dar ce poate fi clasificat ca informații de identificare personală? În mod tradițional, informațiile sensibile, cum ar fi numele complet, numărul de securitate socială, permisul de conducere, adresa poștală sau informațiile despre cardul de credit au fost considerate PII. În cele din urmă, au fost incluse și informații mai puțin sensibile, cum ar fi coduri poștale, adrese IP sau ID-uri de conectare. În timp, amprenta ta digitală, adică datele pe care le lași în urmă ca urmare a navigării pe internet, ar putea ajunge să includă unele dintre acestea.

Bitdefender Digital Identity Protection reprezintă calea privată către libertatea online, permițându-vă să recâștigați controlul asupra vieții digitale. Și necesită doar numele dvs., cea mai utilizată adresă de e-mail și numărul dvs. de telefon. Pe baza acestora, caută atât pe Surface Web, cât și pe Dark Web informații personale care au fost expuse public.

Bitdefender Digital Identity Protection oferă următoarele:

- **Servicii de monitorizare și detecție:** monitorizează mai mult de 100 de informații de identificare personală, cum ar fi SSN, cărți de credit sau adresa de domiciliu și afișează toate datele găsite despre amprenta dvs. online.

  > **Notă**
  > Bitdefender nu stochează și nu procesează informații de identificare personală. Sunt păstrate doar referințele la posibile încălcări ale datelor, fără a include datele sensibile.

- **Alerte în timp real:** Primiți notificări despre încălcări ale datelor și date expuse în Dark Web, informații personale în Surface Web și potențiali imitatori ai dvs. pe rețelele sociale.

- **Solutii:** Serviciul nostru sugerează acțiuni clare necesare pentru a rezolva problemele și oferă mementouri dacă o problemă nu este rezolvată în întregime. De asemenea, poate oferi instrucțiuni despre cum să eliminați anunțurile personalizate, să vă exportați datele sau să dezactivați urmărirea.

9.2. Noțiuni de bază

9.2.1. Activați Protecția identității digitale

Activați abonamentul Bitdefender Digital Identity Protection după ce comanda dvs. este plasată și plătită.

1. Deschideți e-mailul de confirmare primit la scurt timp după finalizarea comenzii și faceți clic pe**INCEPE**.
2. Veți fi redirecționat cătrehttps://central.bitdefender.com.
   Conectați-vă cu contul dvs. Bitdefender Central. Dacă nu aveți un cont, alegeți să creați unul.
3. După conectare, abonamentul va fi atașat automat la contul dvs. Central și va declanșa procesul de onboarding.

Alternativ:

- accesează**Abonamentele mele**panoul din Central, situat în partea stângă a ferestrei și faceți clic**+ Activați cu cod**.
- introduceți cheia cu 10 cifre găsită în e-mailul de confirmare și apăsați**ACTIVATI**.
- dacă vi se solicită, selectați cum doriți să utilizați codul, apoi faceți clic pe**ACTIVATI**.

9.2.2. Configurați protecția identității digitale

1. Mergi la https://central.bitdefender.com/ și conectați-vă la contul dvs.
   Dacă nu aveți deja un cont, faceți clic pe **CREEAZĂ CONT**, apoi introduceți numele dvs. complet, o adresă de e-mail și o parolă.
2. Selectați panoul Digital Identity Protection.
   Este afișat un ecran de întâmpinare.
3. Clic **ÎNCEPE**.
4. Acum veți fi informat cu privire la informațiile pe care trebuie să le furnizați. Datele dvs. vor fi întotdeauna criptate și securizate.

Clic **URMĂTORUL**.

5. Introduceți prenumele, al doilea nume (dacă există) și numele de familie în casetele corespunzătoare, apoi faceți clic **URMĂTORUL**.
6. Introdu adresa ta de e-mail, apoi dă clic **URMĂTORUL**.
   Asigurați-vă că este o adresă de e-mail validă pe care o puteți accesa.
7. Un cod de securitate este trimis la adresa pe care ați furnizat-o.
   Deschideți e-mailul, copiați codul și inserați-l în câmpul corespunzător.
   După aceea, faceți clic **VERIFICA**.
8. Selectați țara și introduceți numărul de telefon, apoi faceți clic **URMĂTORUL**.
9. Ar trebui să primiți un cod de securitate la scurt timp după aceea.
   Introdu codul, apoi selectează **VERIFICA**.
10. După efectuarea verificării inițiale, faceți clic **FINALIZAREA**.

.

> **Notă**
> Veți fi informat dacă în timpul acestei prime verificări sunt descoperite încălcări, informații de identificare personală sau potențiale tentative de uzurpare a identității.

Protecția identității digitale Bitdefender este acum configurată.

9.2.3. Examinați-vă amprenta digitală, încălcările de date și posibilele uzurpare a identității

După ce finalizați configurarea, Bitdefender Digital Identity Protection efectuează o verificare online pentru a descoperi potențiale uzurpare de identitate, încălcări ale datelor și informații de identificare personală pe Open Web. Vă recomandăm să revizuiți fiecare informație inclusă în **AMRENTA DIGITALĂ**, **SCURGERI DE DATE** și **VERIFICAREA IMPERSONAREA** file.

- Revizuirea amprentei tale digitale (pagina 286)
- Examinarea încălcării datelor (pagina 287)
- Examinarea posibilelor uzurpare a identității (pagina 288)

9.2.4. Îmbunătățiți-vă controlul

Folosim datele pe care le furnizați pentru a monitoriza Surface Web și Dark Web pentru a detecta orice activitate care v-ar putea afecta confidențialitatea sau reputația mărcii dumneavoastră personale.

Dacă doriți să adăugați o altă adresă de e-mail sau un alt număr de telefon, faceți clic ⊕, apoi faceți clic pe **ADĂUGAȚI ADRESA DE E-MAIL** sau **ADAUGA NUMARUL DE TELEFON** și urmați instrucțiunile.

9.3. Bord

Tabloul de bord reunește informațiile incluse în **AMRENTA DIGITALĂ**, **SCURGERI DE DATE** și **VERIFICAREA IMPERSONAREA** secțiuni.

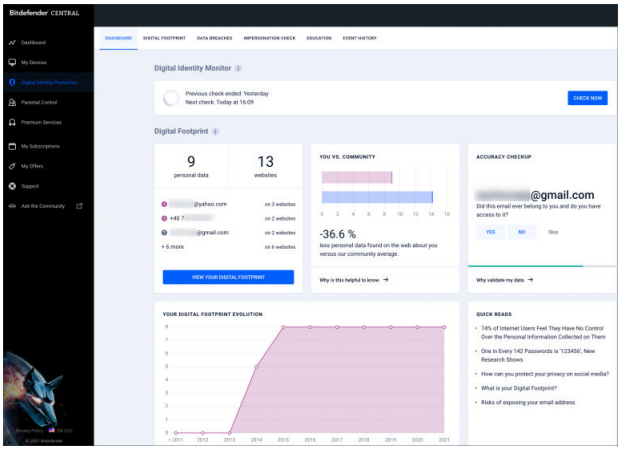
Acesta include următoarele:

- Datele expuse și sursele lor web
- Cantitatea medie de date expuse pentru întreaga comunitate
- Evoluția ta amprentă digitală
- Conținut legat de confidențialitate
- Scurgeri de date
- Numărul mediu de încălcări ale datelor în cadrul comunității

9.3.1. Monitor de identitate digitală

Folosind numai informații exacte, sistemul Bitdefender caută noi date personale expuse pe Open Web și Dark Web și scanează toate platformele principale de rețele sociale pentru orice semne ale unei încercări de uzurpare a identității.

Click pe **VERIFICA ACUM** pentru a efectua o scanare online.



9.4. Amprenta digitală

Informațiile dvs. de identificare personală și sursele acestora apar aici. Depinde de dvs. să evaluați dacă a avea informații publice pe web reprezintă o amenințare.

Monitorul nostru bazat pe inteligență artificială se bazează în mare măsură pe date corecte pentru a detecta noile amenințări, așa că vă rugăm să ne spuneți dacă informațiile sunt corecte sau inexacte.

Odată ce confirmați că o informație este a dvs., o adăugăm la sistemul nostru de monitorizare și îmbunătățim șansele de a descoperi altele în viitor.

9.4.1. Revizuirea amprentei tale digitale

Pentru a vă revizui amprenta digitală:

1. Du-te la **AMRENTA DIGITALĂ** fila.
2. Informațiile care nu au fost încă verificate vor apărea împreună cu textul **Verifica** pe drumul cel bun. Clic **Verifica**, apoi selectați Da sau Nu, în funcție de caz.

> **Notă**
> Fiecare informație confirmată este adăugată la algoritmul nostru de monitorizare, îmbunătățind rezultatele afișate de serviciile noastre. Informațiile care sunt respinse nu vor mai fi afișate. Cu toate acestea, va rămâne disponibil pe web.

9.5. Scurgeri de date

Încălcări apar atunci când hackerii reușesc să ocolească măsurile de securitate ale unei companii și să obțină informațiile tale personale, pentru a le vinde pe dark web. În mod obișnuit, infractorii cibernetici vizează datele de conectare, informațiile de identificare personală (PII), dosarele medicale și detaliile bancare.

Orice organizație sau serviciu poate cădea victima unei încălcări a datelor, dar cei cu o bază mare de consumatori fac ținte mai atractive. Încălcările includ în mod obișnuit nume, adrese de e-mail, nume de utilizator, parole, adrese poștale, numere de telefon, numere de securitate socială (SSN) și datele cărților de credit (număr, data expirării, CVV).

9.5.1. Examinarea încălcării datelor

Pentru a examina încălcările dvs. de date:

1. Du-te la **SCURGERI DE DATE** fila.
2. Sub unele intrări, veți găsi o listă de acțiuni necesare pentru securizarea contului dvs. După efectuarea unei acțiuni, faceți clic pe caseta de lângă ea pentru a confirma.
   Dacă nu sunteți sigur despre cum să efectuați o sarcină, puteți oricând să faceți clic pe linkul inclus în descrierea sarcinii și veți fi redirecționat către o pagină unde veți găsi toți pașii necesari.
   Nu toate încălcările pot fi tratate în acest mod. Unele dintre ele, cum ar fi **Colecția #1**, nu va include pași. În schimb, veți fi redirecționat către articolele disponibile online, unde puteți găsi mai mult ajutor.

   Notă
   Bitdefender nu stochează și nu prelucrează informații de identificare personală. Sunt păstrate doar referințele la posibile încălcări ale datelor, fără a include datele sensibile.

9.6. Verificare uzurpare a identității

Criminalii cunoscuți sub numele de „pretexteri” folosesc arta usurării identității în multe feluri, jucând rolul unei persoane de încredere pentru a-și înșela victimele și pentru a obține acces la informații sensibile. Practica „pretextului” este definită ca prezentarea pe sine ca altcineva pentru a manipula un destinatar pentru a furniza date sensibile, cum ar fi parole, numere de card de credit sau alte informații confidențiale.

Bitdefender Digital Identity Protection monitorizează 25 de platforme de social media și vă anunță instantaneu dacă găsește un profil care ar putea fi o tentativă de uzurpare a identității.

9.6.1. Examinarea posibilelor uzurpare a identității

The **VERIFICAREA IMPERSONAREA** fila este locul în care vor fi afișate toate încercările posibile. Pentru fiecare detectare, puteți alege una dintre cele trei posibilități:

- Este o încercare de uzurpare a identității
- Este propriul tău profil
- Este un alt profil

În funcție de alegere, Bitdefender Digital Identity Protection va recomanda pași specifici pentru a rezolva problema. De fiecare dată când parcurgeți un pas, îl puteți marca ca **Terminat**.

9.7. Educație

Fila Educație servește ca bază de cunoștințe unde utilizatorul poate găsi mai multe informații despre cum să își protejeze identitatea digitală.

Articolele enumerate aici pot fi sortate în mai multe categorii:

- Încălcări
- Expuneri
- Verificare uzurpare a identității

Pentru a accesa versiunea completă a unui articol, faceți clic pe corespunzătoare acestuia **Citeşte mai mult** legătură.

9.8. Istoricul evenimentelor

Secțiunea Istoricul evenimentelor este mijlocul prin care comunicăm constant cu utilizatorii noștri. Reprezintă o listă ordonată cronologic de evenimente privind protecția Identității tale Digitale.

Pe lângă noile amenințări detectate (dacă există), puteți reveni la această pagină pentru sfaturi valoroase despre cum să vă comportați corect online, pentru a crește șansele de a nu rezolva problemele de confidențialitate.

În secțiunea Istoricul evenimentelor, puteți găsi următoarele informații:

- Acțiuni efectuate
- Actualizări de servicii
- Scurgeri de date

10. OBȚINE AJUTOR

10.1. Solicitarea ajutorului

Bitdefender le oferă clienților săi un serviciu rapid și precis de asistență, la un nivel inegalabil. Dacă întâmpini probleme sau dacă ai întrebări legate de produsul tău Bitdefender, poți utiliza o serie de resurse online pentru a identifica o soluție sau un răspuns. De asemenea, poți contacta echipa Serviciului de asistență pentru clienți. Reprezentanții noștri îți vor răspunde la întrebări în timp util și îți vor oferi sprijinul de care ai nevoie.

10.2. 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:
  https://www.bitdefender.ro/consumer/support/
- Comunitatea de experți Bitdefender:
  https://community.bitdefender.com/ro
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare referitoare la securitatea informatică, produsele și compania Bitdefender.

10.2.1. 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 amenințărilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Bitdefender Support Center este pusă la dispoziția publicului. Această multitudine de informații reprezintă încă o cale de a oferi clienților BitDefender asistența tehnică de care au nevoie. Toate cererile valide de

informații sau rapoarte despre bug-uri venind de la clienții BitDefender ajung în cele din urmă în Bitdefender Support Center, ca rapoarte asupra eliminării bug-urilor, fișe de lucru sau articole informative pentru a suplimenta fișierele de suport ale produsului.

Centrul de asistență Bitdefender este disponibil oricând la următoarea adresă: https://www.bitdefender.ro/consumer/support/.

10.2.2. Comunitatea de experți Bitdefender

Comunitatea de experți este un mediu în care utilizatorii, pasionații și fanii Bitdefender pot interacționa, face schimb de idei, se pot ajuta reciproc și își pot împărtăși cunoștințele și soluțiile. De asemenea, acesta este un loc în care se nasc idei și de unde echipele noastre de dezvoltare pot obține un feedback valoros. Membrii comunității sunt utilizatori Bitdefender cu experiență, dornici să-și ajute colegii, în timpul liber. Cu contribuția lor impresionantă și prin eforturi voluntare sincere, am creat o bază de cunoștințe unde utilizatorii pot găsi răspunsuri și îndrumări, prin interacțiune.

Aici veți găsi conversații relevante cu persoane care utilizează Bitdefender pe dispozitivele lor. Comunitatea oferă o legătură reală cu membrii noștri și îți permite să te faci auzit. Este un loc unde ești încurajat să participi, având siguranța că opinia și aportul tău sunt respectate și prețuite. Pentru că activitatea noastră este apreciată, depunem eforturi pentru a asigura o asistență rapidă și precisă, la un nivel incomparabil, și ne dorim să-i aducem pe utilizatorii noștri mai aproape de noi. Cu acest scop în minte, am creat această comunitate.

Accesează pagina Comunității noastre de experți aici:

https://community.bitdefender.com/ro

10.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia conține toate informațiile de care ai nevoie despre cele mai noi amenințări cibernetice. Acesta este locul unde experții Bitdefender își împărtășesc sfaturi și recomandări despre cum să se protejeze împotriva hackerilor, breșelor de securitate a datelor, furtului de identitate și încercărilor de asumare a identității.

Accesează pagina Bitdefender Cyberpedia aici:

https://www.bitdefender.com/cyberpedia/.

10.3. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. Din 2001, BITDEFENDER și-a stabilit o reputație incontestabilă prin străduința constantă pentru o mai bună comunicare, astfel încât să depășească așteptările clienților și partenerilor noștri. Dacă aveți întrebări, nu ezitați să ne contactați direct prin intermediul nostru Centrul de asistență Bitdefender (pagina 290).

https://www.bitdefender.ro/consumer/support/

10.3.1. 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. Mergi la https://www.bitdefender.com/partners/partner-locator.html.
2. Selectează țara și orașul folosind opțiunile corespunzătoare.

GLOSAR

Cod de activare

Este o cheie unică ce poate fi cumpărată de la distribuitorii retail și folosită pentru a activa un anumit produs sau serviciu. Codul de activare permite activarea unui abonament valabil pentru o anumită perioadă de timp și un anumit număr de dispozitive și poate fi, de asemenea, folosit pentru prelungirea unui abonament, cu condiția ca acesta să fie generat pentru același produs sau serviciu.

ActiveX

ActiveX este un model de scriere a programelor, astfel încât alte programe și sistemul de operare să le poată apela. Tehnologia ActiveX este utilizată cu Microsoft Internet Explorer pentru a crea pagini web interactive care arată și se comportă ca niște programe de calculator, mai degrabă decât ca pagini statice. Cu ActiveX, utilizatorii pot pune sau răspunde la întrebări, pot folosi butoane și pot interacționa în alte moduri cu pagina web. Controalele ActiveX sunt adesea scrise folosind Visual Basic. Active X se remarcă prin lipsa completă a controalelor de securitate; experții în securitatea computerelor descurajează utilizarea acestuia pe internet.

Amenințare persistentă avansată

Amenințarea persistentă avansată (APT) exploatează vulnerabilitățile sistemelor pentru a fura informații importante pentru a le livra la sursă. Grupurile mari, cum ar fi organizațiile, companiile sau guvernele, sunt vizate de această amenințare. Obiectivul unei amenințări persistente avansate este de a rămâne nedetectat pentru o lungă perioadă de timp, putând monitoriza și aduna informații importante fără a deteriora mașinile vizate. Metoda folosită pentru a injecta amenințarea în rețea este printr-un fișier PDF sau un document Office care arată inofensiv, astfel încât fiecare utilizator să poată rula fișierele.

Adware

Adware-ul este adesea combinat cu o aplicație gazdă care este furnizată gratuit, atâta timp cât utilizatorul este de acord să accepte adware-ul. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord cu un acord de licență care precizează scopul aplicației, nu se comite nicio infracțiune. Cu toate acestea, reclamele pop-up pot deveni o supărare și, în unele cazuri, pot degrada performanța

sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le colectează pot cauza probleme de confidențialitate pentru utilizatorii care nu cunoșteau pe deplin termenii din acordul de licență.

Arhiva

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.

Ușa din spate

O gaură în securitatea unui sistem lăsată în mod deliberat de proiectanți sau întreținători. Motivația pentru astfel de găuri nu este întotdeauna sinistră; unele sisteme de operare, de exemplu, ies din cutie cu conturi privilegiate destinate utilizării de către tehnicienii de service pe teren sau programatorii de întreținere ai furnizorului.

Sectorul de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (dimensiunea sectorului, dimensiunea clusterului și așa mai departe). Pentru discurile de pornire, sectorul de boot conține și un program care încarcă sistemul de operare.

Virus de pornire

O amenințare care infectează sectorul de pornire al unui disc fix sau al unei dischete. O încercare de pornire de pe o dischetă infectată cu un virus din sectorul de boot va face ca amenințarea să devină activă în memorie. De fiecare dată când porniți sistemul din acel moment, veți avea amenințarea activă în memorie.

botnet

Termenul „botnet” este compus din cuvintele „robot” și „rețea”. Rețelele bot sunt dispozitive conectate la internet infectate cu amenințări și pot fi folosite pentru a trimite e-mailuri spam, a fura date, a controla de la distanță dispozitive vulnerabile sau a răspândi programe spyware, ransomware și alte tipuri de amenințări. Obiectivul lor este de a infecta cât mai multe dispozitive conectate, precum PC-uri, servere, dispozitive mobile sau IoT aparținând marilor companii sau industrii.

Browser

Prescurtare pentru browser web, o aplicație software folosită pentru a localiza și afișa pagini web. Printre browserele populare se numără Microsoft Internet Explorer, Mozilla Firefox și Google Chrome. Acestea

sunt browsere grafice, ceea ce înseamnă că pot afișa atât grafică, cât și text. În plus, majoritatea browserelor moderne pot prezenta informații multimedia, inclusiv sunet și video, deși necesită plug-in-uri pentru unele formate.

Atac de forță brută

Atacul de ghicire a parolei folosit pentru a pătrunde într-un sistem computerizat prin introducerea de combinații posibile de parole, de cele mai multe ori începând cu parola cel mai ușor de ghicit.

Linie de comanda

Într-o interfață de linie de comandă, utilizatorul tastează comenzi în spațiul oferit direct pe ecran folosind limbajul de comandă.

Cookie-uri

În industria internetului, cookie-urile sunt descrise ca fișiere mici care conțin informații despre computere individuale care pot fi analizate și utilizate de agenții de publicitate pentru a urmări interesele și gusturile dvs. online. În acest domeniu, tehnologia cookie-urilor este încă în curs de dezvoltare și intenția este de a direcționa anunțurile direct către ceea ce ați spus că sunt interesele dvs. Este o sabie cu două tăișuri pentru mulți oameni, deoarece, pe de o parte, este eficientă și pertinentă, deoarece vedeți doar reclame despre ceea ce vă interesează. Pe de altă parte, implică de fapt „urmărirea” și „urmărirea” unde mergeți și pe ce dai click. De înțeles, există o dezbatere asupra confidențialității și mulți oameni se simt jigniți de ideea că sunt priviți ca un „număr SKU” (știți, codul de bare de pe spatele pachetelor care este scanat la linia de check-out de la băcănie) . Deși acest punct de vedere poate fi extrem, în unele cazuri este precis.

Hărțuirea cibernetică

Când colegii sau străinii comit acte abuzive împotriva copiilor intenționat pentru a-i răni fizic. Pentru a dăuna emoțional, agresorii trimit mesaje răutăcioase sau fotografii nemăgulitoare, făcând astfel victimele lor să se izoleze de ceilalți sau să se simtă frustrate.

Dicționar Attack

Atacurile de ghicire a parolelor erau folosite pentru a pătrunde într-un sistem informatic prin introducerea unei combinații de cuvinte comune pentru a genera parole potențiale. Aceeași metodă este folosită pentru a ghici cheile de decriptare ale mesajelor sau documentelor criptate.

Atacurile de dicționar reușesc, deoarece mulți oameni înclină să aleagă parole scurte și simple, care sunt ușor de ghicit.

Unitate disc

Este o mașină care citește și scrie date pe un disc. Un hard disk citește și scrie hard disk-uri. O unitate de dischetă accesează dischetele. Unitățile de disc pot fi fie interne (găzduite într-un computer), fie externe (găzduite într-o cutie separată care se conectează la computer).

Descarca

Pentru a copia date (de obicei un fișier întreg) de la o sursă principală pe un dispozitiv periferic. Termenul este adesea folosit pentru a descrie procesul de copiere a unui fișier dintr-un serviciu online pe propriul computer. Descărcarea se poate referi și la copierea unui fișier de pe un server de fișiere din rețea pe un computer din rețea.

E-mail

Poștă electronică. Un serviciu care trimite mesaje pe computere prin rețele locale sau globale.

Evenimente

O acțiune sau o apariție detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi clic pe un buton al mouse-ului sau apăsarea unei taste, sau apariții ale sistemului, cum ar fi epuizarea memoriei.

Exploatările

O modalitate de a profita de diferite erori sau vulnerabilități care sunt prezente într-un computer (software sau hardware). Astfel, hackerii pot obține controlul asupra computerelor sau rețelelor.

Fals pozitiv

Apare atunci când un scaner identifică un fișier ca fiind infectat, când de fapt nu este.

Extensie de nume de fișier

Porțiunea dintr-un nume de fișier, care urmează punctului final, care indică tipul de date stocate în fișier. Multe sisteme de operare folosesc extensii de nume de fișiere, de exemplu Unix, VMS și MS-DOS. Acestea sunt de obicei de la una la trei litere (unele sisteme de operare vechi triste nu acceptă mai mult de trei). Exemplele includ „c” pentru codul sursă C, „ps” pentru PostScript, „txt” pentru text arbitrar.

Euristică

O metodă bazată pe reguli de identificare a noilor amenințări. Această metodă de scanare nu se bazează pe baza de date cu informații despre amenințări specifice. Avantajul scanării euristice este că nu este păcălit de o nouă variantă a unei amenințări existente. Cu toate acestea, poate raporta ocazional cod suspect în programele normale, generând așa-numitul „fals pozitiv”.

Borcan cu miere

Un sistem informatic momeală creat pentru a atrage hackerii să studieze modul în care acționează şi să identifice metodele eretice pe care le folosesc pentru a colecta informații despre sistem. Companiile și corporațiile sunt mai interesate de implementarea și utilizarea honeypot-urilor pentru a-și îmbunătăți starea generală de securitate.

IP

Internet Protocol - Un protocol rutabil din suita de protocoale TCP/IP care este responsabil pentru adresarea IP, rutarea și fragmentarea și reasamblarea pachetelor IP.

applet Java

Un program Java care este proiectat să ruleze numai pe o pagină web. Pentru a utiliza un applet pe o pagină web, trebuie să specificați numele applet-ului și dimensiunea (lungime și lățime, în pixeli) pe care le poate utiliza applet-ul. Când pagina web este accesată, browserul descarcă appletul de pe un server și îl rulează pe computerul utilizatorului (clientul). Appleturile diferă de aplicații prin faptul că sunt guvernate de un protocol de securitate strict.

De exemplu, chiar dacă aplicațiile rulează pe client, acestea nu pot citi sau scrie date pe computerul clientului. În plus, applet-urile sunt restricționate în continuare, astfel încât să poată citi și scrie numai date de pe același domeniu din care sunt servite.

Keylogger

Un keylogger este o aplicație care înregistrează orice tastați. Keylogger-urile nu sunt rău intenționate în natură. Ele pot fi folosite în scopuri legitime, cum ar fi monitorizarea angajaților sau a activității copiilor. Cu toate acestea, acestea sunt din ce în ce mai folosite de infractorii cibernetici în scopuri rău intenționate (de exemplu, pentru a colecta date private, cum ar fi datele de conectare și numerele de securitate socială).

Virus macro

Un tip de amenințare informatică care este codificată ca macrocomandă încorporată într-un document. Multe aplicații, cum ar fi Microsoft Word și Excel, acceptă limbaje macro puternice. Aceste aplicații vă permit să încorporați o macrocomandă într-un document și să executați macrocomandă de fiecare dată când documentul este deschis.

Client de mail

Un client de e-mail este o aplicație care vă permite să trimiteți și să primiți e-mail.

Memorie

Zone de stocare internă în computer. Termenul de memorie identifică stocarea de date care vine sub formă de cipuri, iar cuvântul stocare este folosit pentru memoria care există pe benzi sau discuri. Fiecare computer vine cu o anumită cantitate de memorie fizică, denumită de obicei memorie principală sau RAM.

Non-euristic

Această metodă de scanare se bazează pe baza de date cu informații despre amenințări specifice. Avantajul scanării non-euristice este că nu este păcălit de ceea ce ar putea părea a fi o amenințare și nu generează alarme false.

Prădători online

Persoane care caută să atragă minori sau adolescenți în conversații cu scopul de a-i implica în activități sexuale ilegale. Rețelele de socializare sunt locul ideal în care copiii vulnerabili pot fi vânați cu ușurință și seduși să comită activități sexuale, online sau față în față.

Programe pline

Un fișier într-un format de compresie. Multe sisteme de operare și aplicații conțin comenzi care vă permit să împachetați un fișier astfel încât să ocupe mai puțină memorie. De exemplu, să presupunem că aveți un fișier text care conține zece caractere spațiale consecutive. În mod normal, acest lucru ar necesita zece octeți de stocare.

Cu toate acestea, un program care împachetează fișiere ar înlocui caracterele de spațiu cu un caracter special din seria spațială, urmat de numărul de spații înlocuite. În acest caz, cele zece spații ar necesita doar doi octeți. Aceasta este doar o tehnică de ambalare - sunt multe altele.

Cale

Indicațiile exacte către un fișier de pe un computer. Aceste direcții sunt de obicei descrise prin intermediul sistemului ierarhic de evidență de sus în jos.

Ruta dintre oricare două puncte, cum ar fi canalul de comunicații între două computere.

Phishing

Acțiunea de a trimite un e-mail unui utilizator care pretinde în mod fals că este o întreprindere legitimă stabilită în încercarea de a înșela utilizatorul pentru a renunța la informații private care vor fi folosite pentru furtul de identitate. E-mailul îl direcționează pe utilizator să viziteze un site web unde i se cere să actualizeze informații personale, cum ar fi parolele și numerele de card de credit, de securitate socială și de cont bancar, pe care organizația legitimă le are deja. Totuși, site-ul web este fals și creat doar pentru a fura informațiile utilizatorului.

Foton

Photon este o tehnologie Bitdefender inovatoare, neitruzivă, proiectată pentru minimizarea impactului soluției tale de securitate asupra performanțelor. Prin monitorizarea în fundal a activității PC-ului tău, creează modele de utilizare care vor ajuta la optimizarea pornirii și a proceselor de scanare.

Virus polimorf

O amenințare care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, astfel de amenințări sunt greu de identificat.

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 endpoint către o conexiune logică. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Ransomware

Ransomware este un program periculos care încearcă să obțină bani de la utilizatori prin blocarea sistemelor vulnerabile. CryptoLocker, CryptoWall și TeslaWall sunt doar câteva variante care vânează sistemele personale ale utilizatorilor.

Infecția se poate extinde prin accesarea mesajelor spam, descărcarea atașamentelor e-mail sau instalarea de aplicații, fără ca utilizator să afle ce se întâmplă pe sistemul său. Utilizatorii și companiile sunt vizate zilnic de către hackerii ransomware.

Fișier 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.

Rootkit

Un rootkit este un set de instrumente 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 instrumente 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, conectări și jurnale. Acestea pot, de asemenea, să intercepteze date de la terminale, conexiuni la rețea sau dispozitive periferice, 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 amenințări sau prezența intrușilor în sistem. În combinație cu amenințările, 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.

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 o amenințare de tip cal troian este legată de 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.

Elemente de pornire

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.

Abonament

Contractul de cumpărare care acordă utilizatorului dreptul de a folosi un anumit produs sau serviciu pe un anumit număr de dispozitive și o anumită perioadă de timp. Un abonament expirat poate fi reînnoit automat folosind informațiile furnizate de utilizator la prima achiziție.

Zona de notificare

Introdusă odată cu apariția sistemului Windows 95, bara de sistem se află 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 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.

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.

Amenințare

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 amenințărilor se pot și înmulți. Toate amenințările informatice sunt create de om. O simplă amenințare care poate realiza copii ale sale este relativ simplu de produs. Chiar și o asemenea amenințare este periculoasă întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. O amenințare și mai periculoasă este cea care este capabilă să se răspândească în rețea și poate să treacă de sistemele de securitate.

Actualizare informații despre amenințări

Modelul binar al unei amenințări, utilizat de către soluția de securitate pentru detectarea și eliminarea amenințării.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de programele malițioase și viermi, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cele mai mascate tipuri de amenințări de tip cal troian este un program care pretinde că elimină amenințările de pe calculatorul tău, însă, în loc de aceasta, introduce amenințări pe calculatorul tău.

Termenul provine de la o poveste din opera „Iliada” a lui Homer, în care grecii le 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.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. Rutinele de instalare a actualizărilor verifică dacă pe calculatorul tău există instalată o altă versiune mai veche; dacă nu, nu vei putea instala actualizarea.

Bitdefender dispune de o funcție proprie de actualizare care îți permite să verifici manual actualizările sau să permiți actualizarea automată a produsului.

Virtual Private Network (VPN)

Este o tehnologie care permite o conexiune directă temporară și criptată la o anumită rețea prin intermediul unei rețele mai puțin sigure. Astfel, trimiterea și primirea de date este sigură și criptată, dificil de interceptat de către curioși. O dovadă de securitate este autentificarea, care se poate efectua numai folosind un nume de utilizator și o parolă.

Vierme

Reprezintă un program care se auto-propagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.