GHIDUL UTILIZATORULUI

Bitdefender CONSUMER SOLUTIONS

Password Manager

Bitdefender Password Manager

Ghidul utilizatorului

Data publicării 06.09.2023

Aviz juridic

Bitdefender

Cuprins

DESPRE ACEST GHID

Scopul și publicul țintă

Acest ghid este destinat tuturor utilizatorilor Bitdefender pe toate sistemele de operare compatibile (Windows, MacOS, Android, iOS) care au ales Bitdefender Password Manager ca instrumentul preferat pentru gestionarea parolelor. Informațiile prezentate în acest manual sunt adecvate atât specialiștilor în computere, cât și tuturor celorlalți utilizatori, fiind un ghid accesibil și ușor de înțeles.

Acest ghid te va ajuta să afli cum să valorifici la maximum instrumentul nostru pentru gestionarea parolelor, care oferă un grad înalt de siguranță și numeroase caracteristici, abordând în detaliu toate caracteristicile și funcțiile acestuia.

Îți dorim o lectură plăcută și utilă.

Cum să folosiți acest ghid

Acest ghid este organizat în mai multe teme majore:

Introducere (pagina 5)

Inițiază procesul de instalare și începe să utilizezi Bitdefender Password Manager.

Caracteristici și funcții (pagina 19)

Află cum să utilizezi Bitdefender Password Manager și toate caracteristicile sale.

Obține ajutor (pagina 30)

Unde să căutați și unde să cereți ajutor în cazul în care apar situații neprevăzute.

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. 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.

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.

1.2. Versiunea gratuită de încercare și versiunile cu plată ale Password Manager

Versiunea gratuită de încercare a Bitdefender Password Manager funcționează, din toate punctele de vedere, exact ca versiunea cu plată a produsului, însă disponibilitatea acesteia va expira după 90 de zile de la activare.

> **Notă**
> Reține că, deși versiunea cu plată a produsului poate fi achiziționată sub forma unui produs individual, abonamentele Bitdefender Premium Security și Bitdefender Ultimate Security includ acces nelimitat la Password Manager.

2. INTRODUCERE

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.

2.1.1. 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.

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.

2.2.1. 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**.

2.2.2. 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.

GET IT ON 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 20).

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.

2.2.3. 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.

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!

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.

3.1. 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 6).

> **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.

4. 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.

4.1. 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**.

4.2. 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.

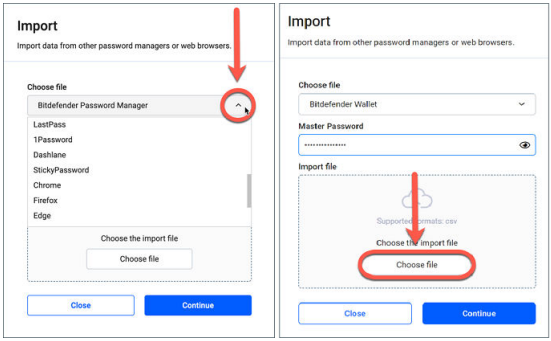
Acum că ai ales Bitdefender Password Manager, vei dori să imporți acele date salvate în această soluție.

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.

4.3. 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.

5. 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.

5.1. Gestionarea parolelor

5.1.1. 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**.

5.1.2. 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.

5.1.3. 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.

5.1.4. 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.

5.1.5. 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.

5.1.6. 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**.

5.2. Gestionarea conturilor

5.2.1. 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.

5.2.2. 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.

5.3. Alte funcționalități

5.3.1. 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**.

5.3.2. 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**.

5.3.3. 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.

5.3.4. 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**.

6. 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.

7. OBȚINE AJUTOR

7.1. 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.

7.2. 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.

7.2.1. 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/.

7.2.2. 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

7.2.3. 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/.

7.3. 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 30).

https://www.bitdefender.ro/consumer/support/

7.3.1. 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 care poate fi cumpărată de la retail și utilizată pentru a activa un anumit produs sau serviciu. Un cod de activare permite activarea unui abonament valabil pentru o anumită perioadă de timp și număr de dispozitive și poate fi folosit și pentru a prelungi un abonament cu condiția 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.

Rețea privată virtuală (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.