MANUALE D'USO

Bitdefender CONSUMER SOLUTIONS

Password Manager

Bitdefender Password Manager

Guida dell'utente

Data di pubblicazione 06/09/2023

Avviso legale

Bitdefender

Indice

INFORMAZIONI SU QUESTA GUIDA

Finalità e destinatari

Questo manuale è rivolto a tutti gli utenti Bitdefender che hanno scelto Bitdefender Password Manager come proprio strumento di gestione delle password per ogni sistema operativo supportato (Windows, MacOS, Android e iOS). È una guida accessibile e consultabile da tutti, non solo agli esperti di computer.

Questo manuale ti aiuterà a scoprire come sfruttare al meglio il nostro password manager ultra sicuro e ricco di funzionalità, descrivendo nei dettagli tutte le sue caratteristiche.

Buona lettura e speriamo che lo troverai utile.

Come usare questo manuale

Questo manuale presenta alcuni argomenti principali:

Come iniziare (pagina 5)

Come iniziare con Bitdefender Password Manager e il processo di installazione.

Caratteristiche e funzionalità (pagina 19)

Scopri come usare Bitdefender Password Manager e tutte le sue funzionalità.

Ottenere aiuto (pagina 31)

Dove cercare e ottenere aiuto in caso di difficoltà o problemi.

Convenzioni usate in questo manuale

Convenzioni tipografiche

Nel manuale vengono usati diversi stili di testo per migliorare la leggibilità. L'aspetto e il significato sono illustrati nella tabella sottostante.

Aspetto	Descrizione
sample syntax	Gli esempi di sintassi vengono stampati con monospaced caratteri.
https://www.bitdefender.com	I link URL indirizzano a una qualche ubicazione esterna, su server http o ftp.
documentation@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo come informazioni di contatto.
A proposito di questa guida (pagina 1)	Questo è un link interno, verso una qualche ubicazione nel documento.
filename	File e directory vengono stampati utilizzando monospaced font.
opzione	Tutte le opzioni del prodotto vengono stampate utilizzando **grassetto** caratteri.
parola chiave	Le parole chiave o le frasi importanti vengono evidenziate utilizzando **grassetto** caratteri.

Avvertenze

Le avvertenze appaiono sotto forma di note di testo, segnalate graficamente, portando alla tua attenzione ulteriori informazioni relative al paragrafo attuale.

Nota

Le note sono solo piccole osservazioni. Anche se si possono omettere, le note potrebbe fornire informazioni preziose, come una determinata caratteristica o un link verso eventuali temi collegati.

Importante

Richiede la tua attenzione e non è consigliato ignorarla. Solitamente, fornisce informazioni non critiche ma importanti.

Avvertimento

Si tratta di un'informazione critica che dovresti trattare con maggiore cautela. Se segui le istruzioni, non accadrà nulla di male. Dovresti leggerla e comprenderla, perché descrive qualcosa di estremamente rischioso.

Richiesta di commenti

Ti invitiamo ad aiutarci a migliorare il presente manuale. Abbiamo provato e verificato tutte le informazioni con la massima attenzione. Ti preghiamo di scriverci per indicarci eventuali errori che dovessi riscontrare nel manuale o suggerirci come poterlo migliorare, per aiutarci a fornirti la migliore documentazione possibile.

Segnalacelo inviando una mail a documentation@bitdefender.com. Scrivi tutte le tue e-mail relative alla documentazione in inglese in modo che possiamo elaborarle in modo efficiente.

1. COS'È BITDEFENDER PASSWORD MANAGER

Bitdefender Password Manager è un servizio multipiattaforma sviluppato per aiutare gli utenti a memorizzare e organizzare tutte le proprie password online. Si basa sui più potenti algoritmi di cifratura noti per il massimo livello di protezione e sicurezza digitale. Funziona come un'estensione del browser e una soluzione app mobile per la gestione di identità e password, dati bancari e qualsiasi altro tipo di informazioni sensibili sui vari dispositivi.

Bitdefender Password Manager può salvare, compilare e generare automaticamente, nonché gestire le tue password per tutti i siti web e i servizi online con l'aiuto di una sola password principale, rendendo così la tua intera identità digitale più facile da gestire.

1.1. Sicurezza e come funziona

Alla base del software {1}{2} ci sono alcuni dei più recenti algoritmi di cifratura che garantiscono la più elevata sicurezza dei dati a cui gli utenti possano aspirare, come AES-256-CCM, SH512, BCRYPT e i protocolli HTTPS e WSS per la trasmissione dei dati. Tutti i dati coinvolti vengono cifrati e decifrati localmente. Ciò fa in modo che solo il titolare dell'account possa avere accesso alle informazioni memorizzate nell'account stesso, nonché alla password principale utilizzata per accedervi, così da poter poi usare i relativi dati.

1.2. Versioni di prova e a pagamento di Password Manager

La versione di prova di Bitdefender Password Manager funziona con tutti gli account proprio come la versione a pagamento del prodotto, ma la sua disponibilità scadrà dopo 90 giorni dall'attivazione.

Nota

Ti ricordiamo che anche se la versione a pagamento del prodotto può essere acquistata come prodotto indipendente, l'accesso illimitato a Password Manager è incluso negli abbonamenti a Bitdefender Premium Security e Bitdefender Ultimate Security.

2. COME INIZIARE

2.1. Requisiti di sistema

È possibile utilizzare la versione più recente di Bitdefender Password Manager solo su dispositivi con i seguenti sistemi operativi:

- **Per gli utenti PC:**
  - Windows 7 con Service Pack 1
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows 11
- **Per gli utenti macOS:**
  - macOS 10.14 (Mojave) e versioni successive

  Nota

  Ricordati che le prestazioni del sistema potrebbero risentirne su dispositivi dotati di CPU di vecchia generazione.
- **Per gli utenti iOS:**
  - iOS 11.0 o versioni successive
- **Per gli utenti Android:**
  - Android 5.1 e versioni successive

  Nota

  - La funzionalità di sblocco con le impronte digitali è supportata da **Android 6.0** e versioni successive.
  - La funzionalità di compilazione automatica è supportata da **Android 8.0** e versioni successive, compatibile con iPhone, iPad e iPod touch.

2.1.1. Requisiti software

Per poter usare Bitdefender Password Manager e tutte le sue funzionalità, i tuoi dispositivi Windows o macOS devono soddisfare i seguenti requisiti software:

- **Microsoft Edge** (basato su Chromium 80 e successivi)
- **Mozilla Firefox** (versione 65 o successiva)
- **Google Chrome** (versione 72 o successiva)
- **Safari** (versione 12 o successiva)

Nota
I requisiti software non sono applicabili per Android e iOS.

Avvertimento
Se i requisiti di sistema indicati sopra non vengono soddisfatti, non sarà possibile installare Bitdefender Password Manager o il prodotto potrebbe non funzionare correttamente.

2.2. Installazione

Questo capitolo ti illustrerà come installare Bitdefender Password Manager sia sul tuo browser web sul tuo PC Windows e macOS, nonché sui tuoi dispositivi mobili Android o iOS.

Importante
Prima dell'installazione, assicurati di avere un abbonamento valido a Password Manager nel tuo account **Bitdefender Central**, così che l'estensione del browser possa recuperarne la validità dal tuo account.

Gli abbonamenti attivi sono indicati nella sezione **I miei abbonamenti** in Bitdefender Central.

2.2.1. Installazione su dispositivi Windows e macOS

A differenza della maggior parte delle applicazioni desktop e dei software che devono essere installati e impostati su questi dispositivi, Bitdefender Password Manager è disponibile come estensione del browser, anche nota come add-on, che può essere aggiunta e attivata nel tuo browser preferito.

I browser attualmente supportati per il prodotto sono: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge** e **Safari**.

1. Vai in https://central.bitdefender.com/ e accedi al tuo account.
   Se non hai già un account, seleziona **CREA ACCOUNT** e inserisci il tuo nome completo, un indirizzo e-mail e una password.
2. Seleziona **I miei dispositivi** nella barra laterale sinistra dello schermo.
3. Nella sezione **I miei dispositivi**, continua selezionando **+ Aggiungi dispositivo**.
4. Si aprirà una nuova finestra. Scegli **Password Manager** nella schermata di selezione.
5. Scegli **questo dispositivo**.
   Se stai cercando di installarlo su un altro dispositivo, seleziona Altri dispositivi. Potrai successivamente inviare un link di download al rispettivo dispositivo o copiare direttamente l'URL per l'installazione.
6. Ora scegli su quale browser vuoi installare l'estensione di Password Manager.
7. Ogni pulsante corrispondente ti reindirizzerà al Negozio delle estensioni del browser. Da qui, segui semplicemente le istruzioni sullo schermo come mostrato di seguito:

   Microsoft Edge

   - Seleziona il pulsante **Ottieni**
   - Seleziona **Aggiungi estensione** nel prompt che compare sullo schermo

   Google Chrome

   - Seleziona il pulsante **Aggiungi a Chrome**
   - Nella casella di conferma, seleziona **Aggiungi estensione**

   Mozilla Firefox

   - Seleziona il pulsante **Aggiungi a Firefox**
   - Seleziona il pulsante **Installa** nell'angolo in alto a destra dello schermo

   Safari

   - Seleziona il pulsante **Ottieni** e seleziona su **Installa**
   - Apri Safari e seleziona **Preferenze** nella barra superiore del menu

- Nella finestra Preferenze, seleziona la scheda **Estensioni**
- Seleziona la casella accanto a Password Manager per attivarlo

Una volta seguiti questi passaggi, imposta una password principale sicura e premi il pulsante **Salva la password principal**e dopo aver letto e accettato i **Termini e le condizioni**.

Importante
Ricordati che la password principale ti servirà per sbloccare tutte le password, i dati delle carte di credito e gli appunti salvati in Bitdefender Password Manager. È la chiave che consente al proprietario di usare il prodotto.

Avvertimento
Dopo aver creato la password principale, riceverai un **codice di recupero di 24 cifre**. **Annota il tuo codice di recupero in un luogo sicuro e non perderlo**. Il codice è l'unico modo per accedere alle tue password salvate in Password Manager nel caso dovessi **dimenticare la password principale** impostata in precedenza per il tuo account.

- Una volta fatto, puoi premere **Chiudi**.

2.2.2. Installazione su dispositivi Android

Il modo più facile per installare Bitdefender Password Manager per telefoni e tablet Android è scaricare l'applicazione direttamente da Google Play.

GET IT ON Google Play

Si può installare la app Bitdefender Password Manager anche tramite il tuo account **Bitdefender Central**:

1. Accedi al tuo account Bitdefender Central sul tuo dispositivo mobile Android tramite https://login.bitdefender.com/central/login.
2. Selezionare **I miei dispositivi** nella barra laterale sinistra dello schermo.
3. Nel **I miei dispositivi** sezione, procedere cliccando su **+ Aggiungi dispositivo**.

4. Questa azione farà apparire una nuova finestra. Scegliere **Gestore di password** nella schermata di selezione.
5. Scegliere **Questo dispositivo**.
   Se stai cercando di installarlo su un altro dispositivo, seleziona **Altri dispositivi**. Potrai successivamente inviare un link di download al rispettivo dispositivo o copiare direttamente l'URL per l'installazione.
6. L'installazione ti reindirizzerà a **Google Play**. Tocca **Installa** per scaricare Bitdefender Password Manager su Android.
7. Una volta completato il download, apri l'applicazione Password Manager.
8. Se non accedi automaticamente al tuo account, fallo inserendo il tuo nome utente e la tua password.
   Dopo aver seguito questi passaggi, imposta una password principale sicura, quindi premi il tasto **Salva password principale** pulsante dopo aver letto e concordato con il **Termini e Condizioni**.

   Importante
   Tieni presente che avrai bisogno di questa password principale per sbloccare tutte le password, le informazioni sulla carta di credito e le note salvate in Bitdefender Password Manager. Questa è essenzialmente la chiave che consente al proprietario di utilizzare questo prodotto.

   Avvertimento
   Dopo aver creato la password principale, riceverai a **Chiave di ripristino a 24 cifre**. Prendi nota della chiave di ripristino in un luogo sicuro e non perderla. Questa chiave è l'unico modo per accedere alle tue password salvate in Password Manager nel caso in cui ti capitasse **dimenticare la password principale** precedentemente impostato per il tuo account.

   ❍ Puoi premere **Vicino** quando fatto.
9. Crea un **PIN di 4 cifre**, così se dovessi passare a un'altra app e poi tornare a Password Manager, non dovrai inserire nuovamente la password principale che hai impostato in precedenza. Se disponibile, potrai anche attivare il riconoscimento facciale o l'autenticazione tramite l'impronta digitale.

10. Tocca **Compilazione automatica** per configurare le impostazioni della compilazione automatica di Android.

> **Nota**
> Se salti questo passaggio, potrai attivare e personalizzare le funzionalità di compilazione automatica di Android successivamente seguendo le istruzioni disponibili in Compilazione automatica intelligente (pagina 20).

11. Ti sarà presentato un elenco di app che possono compilare automaticamente le password.
    Seleziona **Password Manager** e successivamente il dispositivo ti chiederà di confermare se ritieni affidabile questa app.
    Tocca **OK**.

12. Inserisci il PIN impostato nel **passaggio 9** per confermare questa azione.

L'installazione sui tuoi dispositivi Android è ora completata.

2.2.3. Installazione sui dispositivi iOS

Il modo più facile per installare Bitdefender Password Manager per i dispositivi iOS e iPadOS è scaricare l'applicazione da App Store di Apple.

Download on the App Store

L'installazione dell'app Bitdefender Password Manager può essere eseguita anche tramite il tuo Bitdefender centrale account:

1. Sul tuo iPhone o iPad accedi al tuo account Bitdefender Central tramite https://login.bitdefender.com/central/login.
2. Selezionare **I miei dispositivi** nella barra laterale sinistra dello schermo.
3. Nel **I miei dispositivi** sezione, procedere cliccando su **+ Aggiungi dispositivo**.
4. Questa azione farà apparire una nuova finestra. Scegliere **Gestore di password** nella schermata di selezione.
5. Scegliere **Questo dispositivo**.
   Se stai cercando di installare su un dispositivo diverso, seleziona **Altri dispositivi**. È quindi possibile inviare tramite e-mail un collegamento

per il download al rispettivo dispositivo o copiare direttamente l'URL per l'installazione.

6. L'installazione ti reindirizzerà all'**App Store**. Tocca l'icona della nuvola con una freccia che punta verso il basso per scaricare Bitdefender Password Manager per iOS.
7. Una volta che l'applicazione è stata installata, aprila e spunta la piccola casella sulla schermo. Seleziona **Continua** dopo aver letto e accettato l'**Accordo di abbonamento**.
8. Se non accedi automaticamente al tuo account, accedi utilizzando il tuo nome utente e password.
   Dopo aver seguito questi passaggi, imposta una password principale sicura, quindi premi il tasto **Salva password principale** pulsante dopo aver letto e concordato con il **Termini e Condizioni**.

   Importante
   Tieni presente che avrai bisogno di questa password principale per sbloccare tutte le password, le informazioni sulla carta di credito e le note salvate in Bitdefender Password Manager. Questa è essenzialmente la chiave che consente al proprietario di utilizzare questo prodotto.

   Avvertimento
   Dopo aver creato la password principale, riceverai a **Chiave di ripristino a 24 cifre**. Prendi nota della chiave di ripristino in un luogo sicuro e non perderla. Questa chiave è l'unico modo per accedere alle tue password salvate in Password Manager nel caso in cui ti capitasse **dimenticare la password principale** precedentemente impostato per il tuo account.

   ❍ Puoi premere **Vicino** quando fatto.
9. Creare un **PIN a 4 cifre**, quindi se passi a un'altra app e poi torni a Password Manager, non dovrai reinserire la password principale che hai impostato in precedenza. Se disponibile, puoi anche abilitare il riconoscimento facciale o l'autenticazione delle impronte digitali.

L'installazione sul tuo dispositivo iOS / iPadOS è ora completata!

3. PIANO CONDIVISO

Bitdefender Password Manager Shared Plan consente a più utenti di accedere e utilizzare lo stesso abbonamento. Fornisce un approccio centralizzato all'accesso, all'amministrazione e al supporto del software, offrendo una soluzione economica per la condivisione del servizio di password manager tra più utenti.

- Il responsabile del piano di abbonamento condiviso, denominato Responsabile del Piano, può condividere il servizio tra gli iscritti.
- Ogni membro riceve un account Bitdefender Central unico, collegato al proprio indirizzo e-mail e all'accesso al servizio Password Manager.

3.1. Condivisione di Bitdefender Password Manager con più utenti

Invito di membri

Per aggiungere uno o più utenti all'abbonamento condiviso, il gestore del piano deve seguire questi passaggi:

1. Accedere al proprio account Bitdefender Central all'indirizzo https://central.bitdefender.com/.
2. Accedere al menu **I miei abbonamenti** situato sul lato sinistro della pagina.
3. Scegliere **Invita membro** nel pannello **Bitdefender Password Manager Shared Plan**.
4. Inserire l'e-mail di ogni persona con cui si desidera condividere l'abbonamento, quindi fare clic su **Invia**. È possibile aggiungere un massimo di 3 membri alla volta.
5. Le istruzioni per l'installazione vengono inviate subito via e-mail ai nuovi membri. Cliccare su **Chiudi** per uscire dalla finestra di conferma.

Nota

I membri hanno 24 ore per accettare il tuo invito una volta ricevuto via email.

- I membri invitati appariranno con lo stato "Invitato".
- Li vedrai come membri "Attivi" dopo che avranno accettato l'invito. Riceverai inoltre una notifica via e-mail per ogni invito accettato.

Rimozione di membri

L'accesso al piano condiviso di Bitdefender Password Manager viene perso per i membri che vengono rimossi. Quando il gestore del piano decide di rimuovere un membro dell'abbonamento, il membro riceve una notifica via e-mail. Per i 30 giorni successivi, l'ex membro passa a una versione di prova di Bitdefender Password Manager di 30 giorni con tutte le funzionalità. Il servizio verrà poi disattivato.

Il responsabile del piano può eliminare gli utenti dal piano condiviso nel seguente modo:

1. Accedere al proprio account Bitdefender Central all'indirizzo https://central.bitdefender.com/.
2. Accedere al menu **I miei abbonamenti** situato sul lato sinistro della pagina.
3. Nel pannello del **Bitdefender Password Manager Shared Plan**, fare clic su **Gestisci**, quindi scegliere **Modifica membri** nel menu.
4. Fare clic sul pulsante **Rimuovi** per togliere un membro dal piano condiviso.
5. Scegliere **Sì, rimuovi membro** e cliccare sul pulsante **Termina modifica** per rendere effettive le modifiche.

Nota

Quando un membro viene eliminato dal piano condiviso, il suo stato viene modificato in **In attesa di rimozione** fino alla sua completa eliminazione.

Accettare un invito

Riceverai un'e-mail quando qualcuno ti invita a diventare un membro dell'abbonamento al piano condiviso di Bitdefender Password Manager. Hai 24 ore per accettare un invito una volta che ti è stato inviato.

Per accettare l'invito e ottenere l'accesso alle funzionalità del gestore password, l'utente deve seguire questi passaggi:

1. Aprire l'e-mail ricevuta intitolata **[Inizia a usare il tuo abbonamento Bitdefender come membro]** e fare clic sul pulsante **ATTIVA IN CENTRAL**.
2. La pagina Bitdefender Central si aprirà quindi nel tuo browser.
   - Se hai già un account utente Bitdefender associato all'e-mail con cui è stato inviato l'invito, **accedi** per richiedere l'abbonamento condiviso.
   - Se non hai un account utente Bitdefender, clicca su **Crea** e registrati con la stessa e-mail con cui ti è stato inviato l'invito per richiedere l'abbonamento condiviso.
     - Inserisci il tuo nome e cognome
     - Inserisci il tuo indirizzo email
     - Inserisci la tua password
     - Clicca sul pulsante Crea account e sarai iscritto.
3. Dopo aver effettuato l'accesso, fare clic su **Inizia** nella schermata di benvenuto che informa che l'abbonamento a Bitdefender Password Manager è ora attivo.
4. Seguire i passaggi sullo schermo descritti anche in Installazione (pagina 6).

> **Nota**
> L'e-mail del gestore del piano viene visualizzata nel tuo account Bitdefender Central nella parte superiore del menu Password Manager e sulla scheda di abbonamento, sotto I miei abbonamenti.
>
> Se hai bisogno di assistenza con il piano condiviso, contattali.

4. IMPORTARE ED ESPORTARE LE TUE PASSWORD

Bitdefender Password Manager è stato sviluppato in modo tale da facilitare con efficacia la comunicazione e il trasferimento di dati con fonti esterne, piattaforme e strumenti software. Questo è il motivo principale per cui è possibile importare o esportare password da o verso Bitdefender Password Manager con estrema facilità.

4.1. Compatibilità

Bitdefender Password Manager può trasferire facilmente dati dal seguente elenco di applicazioni:

- **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**

> **Nota**
> Se il nome del browser o dello strumento di gestione delle password da cui stai cercando di trasferire i dati non è indicato nell'elenco fornito sopra, puoi seguire la nostra guida online che illustra come modificare un file CSV da un password manager non supportato così da importarne i dati in **Bitdefender Password Manager**: https://www.bitdefender.it/consumer/support/answer/22167/

Questo trasferimento di dati tra Bitdefender Password Manager e altri software di gestione degli account può essere effettuato con i seguenti formati di dati:

CSV, **JSON**, **XML**, **TXT**, **1pif** e **FSK**.

4.2. Importazione in Password Manager

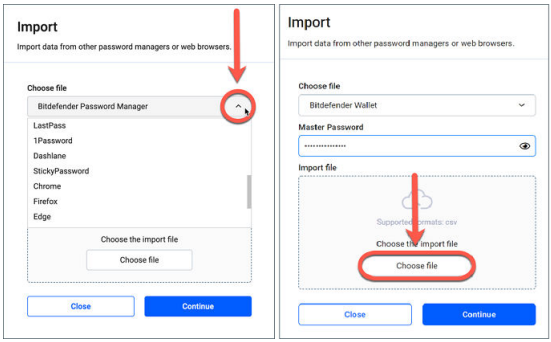
Bitdefender Password Manager ti consente di importare facilmente le password da altri browser e password manager. Se attualmente stai cercando di passare a Bitdefender Password Manager da un altro servizio di gestione delle password, molto probabilmente hai memorizzato una notevole quantità di credenziali, come nomi utente, password e altri dati d'accesso richiesti per tutti i tuoi account.

Ora che hai scelto Bitdefender Password Manager, cercherai d'importarci quei dati salvati.

Ecco come importare le tue informazioni salvate da altre app e browser web in Bitdefender Password Manager, **indipendentemente dal sistema operativo** su cui ha scelto d'installare il prodotto:

1. Seleziona l'icona di Password Manager nel tuo browser web (su Windows o macOS) o lancia l'applicazione di Password Manager (su Android o iOS). Se richiesto, inserisci la tua **password principale**.

2. Apri il menu ☰ di Password Manager per espandere la barra laterale a sinistra e seleziona la voce ⚙ **Impostazioni**.
3. Scorri in basso fino alla sezione **Dati** e seleziona l'opzione **Importa dati**.
4. Usa il menu a discesa per selezionare il nome del browser o della app di gestione delle password da cui vuoi importare i tuoi account. Inserisci la tua **password principale** nel campo corrispondente e seleziona **Scegli file**.



5. Naviga nelle cartelle per trovare il percorso in cui hai salvato il file contenente i tuoi nomi utenti e le tue password, esportato dal tuo attuale browser web o password manager, e premi **Continua**.

Una volta importate, le tue password saranno accessibili su ogni dispositivo in cui è stata installata l'applicazione o l'estensione del browser di Bitdefender Password Manager.

4.3. Esportazione da Password Manager

Bitdefender Password Manager ti consente di esportare facilmente le tue password salvate (incluso le credenziali di accesso per l'account, note protette, ecc.) in un file CSV (valori separati da una virgola) o un file cifrato se vuoi passare a un altro servizio di gestione delle password, così che

la tua partenza da Bitdefender Password Manager non sarà un processo troppo complicato.

> **Importante**
> Un file CSV **non** è cifrato e contiene nomi utenti e password in formato di testo normale, il che significa che le tue informazioni private possono essere lette da chiunque abbia accesso al tuo dispositivo. Ti consigliamo quindi di seguire le istruzioni in basso su un dispositivo affidabile.

Ecco come puoi esportare i tuoi dati da Bitdefender Password Manager:

1. Fai clic sull'icona Password Manager nel tuo browser web (su Windows o macOS) o avvia l'applicazione Password Manager (su Android o iOS). Se richiesto, inserisci il tuo Password principale.
2. Apri il menu di Password Manager per espandere la barra laterale a sinistra e seleziona la voce **Impostazioni**.
3. Scorri in basso fino alla sezione **Dati** e seleziona l'opzione **Esporta dati**.
4. Ora dovresti ricevere le seguenti due opzioni:
   - **CSV**
   - **File protetti da password**

   Seleziona la tua opzione preferita e inserisci la tua password principale, quindi seleziona il pulsante **Esporta dati**.

   > **Nota**
   > Se scegli l'opzione file protetto da password, ti sarà chiesto di cifrare i dati contenenti l'elenco degli account con una password, così che solo tu possa accedervi in caso di necessità.

5. La tua app e/o il tuo browser web procederanno salvando un file chiamato Bitdefender Password Manager_exported_data_current-date nel tuo sistema nella cartella predefinita di download. Contiene tutti i dati memorizzati in Bitdefender Password Manager.

Dopo aver esportato i tuoi dati, potrai caricarli nel password manager che preferisci.

5. CARATTERISTICHE E FUNZIONALITÀ

Questo capitolo ti guiderà attraverso tutte le caratteristiche e le funzionalità di Bitdefender Password Manager, illustrando la loro utilità e come sfruttarle con la massima efficacia.

5.1. Gestione delle password

5.1.1. Generatore di password

La regola d'oro relativa alla sicurezza online è utilizzare sempre sequenze casuali e univoche per ogni servizio che richiede la creazione di un account. Il riutilizzo delle password in più piattaforme è la prima causa di furti d'identità e perdite associate alla sottrazione di un account.

Questa funzionalità aiuta gli utenti con la generazione di password uniche, sicure e complesse per ogni nuovo account che creano online. Ciò elimina la necessità degli utenti di inventare password complesse da soli o fare attenzione a non riutilizzare la stessa password per più account.

Si può accedere a **Password Generator** tramite la scheda in alto nell'interfaccia di Password Manager.

Il generatore può essere impostato per generare password **comprese tra 4 e 32 caratteri**.

Si possono anche specificare le tipologie di caratteri che dovrebbero o non dovrebbero essere presenti nella password generata casualmente spuntando o deselezionando le caselle corrispondenti. **(Minuscole, maiuscole, numeri, caratteri speciali)**

Premendo il pulsante alla destra della password mostrata, il generatore modificherà la password suggerita.

Per usare la password mostrata, premi **Usa la password**, un'azione che salverà la stringa di caratteri nei tuoi appunti.

> **Nota**
> Le tue password generate in precedenza saranno memorizzate temporaneamente nella cronologia delle password, accessibile tramite il pulsante **Cronologia password**.

5.1.2. Acquisizione delle password

Con questa funzionalità di Password Manager, ti sarà chiesto di memorizzare tutte le tue nuove password subito dopo averle create. Password Manager chiederà agli utenti di memorizzare le loro nuove password appena create, in modo che possano essere aggiunte subito all'ambiente ultra sicuro fornito da Bitdefender.

5.1.3. Compilazione automatica intelligente

Bitdefender Password Manager può essere impostato in modo tale da compilare automaticamente tutte le tue credenziali di accesso e le password più importanti. Algoritmi proprietari possono rilevare e pre-compilare le credenziali sui siti web visitati in precedenza, facendo risparmiare tempo agli utenti ogni volta che accedono a un servizio.

1. Su Windows o macOS, clicca sull'icona **Password Manager** nel tuo browser web.

   Su Android o iOS, esegui l'applicazione **Password Manager**.
   Se richiesto, inserisci la tua **password principale**.

2. Apri il menu di Password Manager per espandere la barra laterale sinistra e seleziona la voce **Impostazioni**.

3. Seleziona **Impostazioni dispositivo**.

4. Qui noterai un pulsante che mostra le opzioni **Disattiva compilazione automatica** o **Attiva compilazione automatica**. Questa impostazione controlla lo stato operativo della funzionalità di compilazione automatica intelligente.

5.1.4. Rapporto di sicurezza

Il Rapporto di sicurezza è uno strumento che genererà rapporti basati su un numero di funzionalità pensate per rafforzare la tua sicurezza digitale. Ti farà sapere se una password richiede la tua attenzione immediata determinando il suo livello di sicurezza. Rileverà i duplicati delle password, chiedendoti di modificarle di conseguenza, evitando i pericoli derivanti dal riutilizzare le stesse password per più account.

Il rapporto si concentrerà nel fornire informazioni sull'igiene generale delle password: in particolare se ci sono password duplicate e deboli, o password o indirizzi e-mail trapelati.

Ciò viene fatto confrontando l'elenco degli hash cifrati dalla pagina web di Troy localmente sul tuo dispositivo per verificare se contiene gli hash corrispondenti delle tue password. Se viene trovata una corrispondenza, riceverai un avviso per incoraggiarti a modificare le tue password o altre credenziali d'accesso.

Per accedere al **rapporto di sicurezza**, accedi all'interfaccia di Password Manager e seleziona il suo pulsante corrispondente nella barra superiore.

5.1.5. Sincronizzazione con altre piattaforme

Salvare le tue password una volta in Bitdefender Password Manager ti consentirà di memorizzarle e accedervi in modo sicuro su tutti i tuoi dispositivi Windows, Mac, Android o iOS da Chrome, Safari, Firefox ed Edge o nelle app mobile.

> **Nota**
> Bitdefender è dotato anche di una **modalità offline** per accedere alle tue password nel caso non disponessi momentaneamente di una connessione a Internet. Ciò rende le tue password accessibili in qualsiasi momento e da qualsiasi luogo.

5.1.6. Eliminare una voce

Per eliminare prima le password salvate, premi l'icona di modifica accanto alla voce che vuoi rimuovere, localizzata nella scheda **Account**. Scorri in basso e seleziona **Elimina**. Quando ti viene chiesto, se hai la certezza di voler rimuovere l'account, seleziona **Rimuovi**.

5.2. Gestione dell'account

5.2.1. Autenticazione

L'autenticazione in Bitdefender Password Manager viene fatta attraverso il **PIN** impostato nella fase di installazione del prodotto. (Nota che la funzionalità di **Blocco automatico** bloccherà il password manager o uscirà dopo un periodo di inattività a livello del browser o chiudendo la app mobile)

Inoltre, se disponibili, può essere fatto anche sfruttando alcuni dati biometrici, come l'**impronta digitale** o il **riconoscimento facciale**.

Per **attivare o disattivare** l'autenticazione basata sui dati biometrici:

1. Su Windows o macOS, fai clic su **Password Manager** icona nel tuo browser web.

   Su Android o iOS, avvia il file **Password Manager** applicazione.
   Se richiesto, inserisci il tuo Password principale.

2. Apri il menu Gestore password per espandere la barra laterale a sinistra e fare clic su **Impostazioni** elemento del menu.
3. Clicca su **Impostazioni del dispositivo**.
4. Qui noterai un pulsante che mostra le opzioni **Disattiva dati biometrici** o **Attiva dati biometrici**. Questa impostazione controlla lo stato operativo della funzionalità di autenticazione basata sui dati biometrici.

5.2.2. Reimpostazione della password principale

> **Importante**
> La funzionalità **Cambia password principale** non è disponibile sui dispositivi mobili. L'unico modo per cambiare o recuperare la tua password principale è tramite l'estensione del browser Bitdefender Password Manager su Windows PC o un dispositivo macOS.

Ecco come cambiare la tua **password principale** come misura precauzionale e crearne una nuova in Bitdefender Password Manager:

1. Una volta installata l'estensione del browser, clicca sull'icona **Password Manager** nella barra degli strumenti del browser web.
2. Inserisci la tua attuale password principale per sbloccare il vault.

> **Importante**
> Se non ricordi la tua attuale password principale, seleziona l'opzione **Ho dimenticato la mia password** nella stessa schermata. Inserisci il **codice di recupero di 24 cifre** fornito durante la configurazione iniziale di Bitdefender Password Manager e digita una nuova password principale. **Se hai dimenticato o smarrito** sia la **password principale** che il **codice di recupero**, come ultima possibilità, **contatta un responsabile di Bitdefender per aiutarti a reimpostare il tuo account**. Reimpostare il tuo account **eliminerà tutti i tuoi dati e le tue password** salvati in Bitdefender Password Manager.

3. Apri il menu Gestore password per espandere la barra laterale a sinistra e fare clic su **Impostazioni** elemento del menu.
4. Seleziona il pulsante **Il mio account** nella sezione **Account**.
5. Si aprirà una finestra con alcune informazioni sul tuo abbonamento di Password Manager.
   Seleziona il pulsante **Cambia password principale**.
6. Si aprirà una nuova finestra dove potrai selezionare una nuova password principale. Inserisci la tua attuale password principale e digitane una nuova. La nuova password principale deve contenere un minimo di 8 caratteri, almeno una lettera minuscola, una maiuscola e un numero.
7. Premi il pulsante **Cambia** una volta fatto.
8. Attendi alcuni istanti finché Bitdefender non resetta la vecchia password principale.
   Non uscire dal tuo browser web!
9. Successivamente, ti sarà fornito un nuovo **codice di recupero di 24 cifre**. Annotati il codice di recupero in un posto sicuro e **non perderlo**. Il codice è l'unico modo per accedere alle tue password salvate in Password Manager nel caso avessi dimenticato la password principale.
   Premi **Chiudi** una volta fatto.
10. Sarà effettuata la disconnessione da Bitdefender Password Manager.
    Per sbloccare il vault, usa la nuova password principale che hai appena impostato.

5.3. Altre funzionalità

5.3.1. Gestione delle identità

Questa funzionalità consente agli utenti di memorizzare più identità e permette a Password Manager di compilare automaticamente i dettagli nei moduli web prima di effettuare un acquisto in modo sicuro, facile e veloce.

Come tutto il resto in Password Manager, tutti i dati sensibili contenuti all'interno di queste identità memorizzate sono cifrati e disponibili solo per il dispositivo dell'utente.

Per aggiungere un'identità a Password Manager:

1. Su Windows o macOS, fai clic su **Password Manager** icona nel tuo browser web.

   Su Android o iOS, avvia il file **Password Manager** applicazione.
   Se richiesto, inserisci il tuo Password principale.

2. Apri il menu di Password Manager per espandere la barra laterale sinistra e seleziona la voce **Identità**.
3. Premi il pulsante **Aggiungi identità** in fondo.
4. Completa le informazioni che desideri vengano memorizzate e premi **Salva**.

5.3.2. Gestione delle carte di credito

Questa funzionalità ti consente di salvare e compilare i dati delle carte di credito per un'esperienza di acquisto più facile, veloce e sicura.

Per aggiungere una carta di credito a Password Manager:

1. Su Windows o macOS, fai clic su **Password Manager** icona nel tuo browser web.

   Su Android o iOS, avvia il file **Password Manager** applicazione.
   Se richiesto, inserisci il tuo Password principale.

2. Apri il menu di Password Manager per espandere la barra laterale sinistra e seleziona la voce **Carte di credito**.
3. Premere sul **Aggiungi identità** pulsante in basso.

4. Completare i dettagli che si desidera memorizzare, quindi premere **Salva**.

5.3.3. Proteggimi

La funzionalità Proteggimi ti consente di disconnettersi da remoto o eliminare la cronologia di navigazione di computer, tablet o dispositivi mobili. Se stai condividendo un dispositivo con altre persone, ti consigliamo vivamente di attivare questa funzionalità.

Per localizzare e attivare questa funzionalità:

1. Su Windows o macOS, fai clic su **Password Manager** icona nel tuo browser web.

   Su Android o iOS, avvia il file **Password Manager** applicazione.
   Se richiesto, inserisci il tuo Password principale.

2. Apri il menu di Password Manager per espandere la barra laterale sinistra e seleziona la voce **Proteggimi**.

3. Premi il pulsante **Proteggi tutte le sessioni**.
   Sei stai cercando di proteggere solo un dispositivo in particolare, individualo nell'elenco dei dispositivi su cui è stato installato o attivato su un determinato browser Password Manager.

5.3.4. Note

Secure Notes è una funzionalità che agisce come un taccuino segreto in cui puoi memorizzare dati sensibili, ordinarli e usare una codifica a colori per visualizzarli meglio. Non solo manterrà tutte le informazioni in ordine, ma anche al sicuro.

Per individuare e abilitare questa funzione:

1. Su Windows o macOS, fai clic su **Gestore di password** icona nel tuo browser web.

   Su Android o iOS, avvia il file **Gestore di password** applicazione.
   Se richiesto, inserisci il tuo Password principale.

2. Apri il menu di Password Manager per espandere la barra laterale sinistra e seleziona la voce **Note**.

3. Premi il pulsante **Aggiungi nota**.

Una volta indicate tutte le informazioni che vuoi conservare, premi **Salva**.

6. DOMANDE FREQUENTI

Alcune domande comuni su Bitdefender Password Manager tendono a ripetersi. Noi abbiamo le risposte! Qui potrai scoprire maggiori dettagli sul tuo account Bitdefender, su come importare le password, sui protocolli di sicurezza dei dati e altri argomenti importanti per i nostri clienti.

Domande generali su Bitdefender Password Manager

Come posso bloccare la finestra pop-up di Password Manager nella mia soluzione di sicurezza Bitdefender?

La notifica di Password Manager mostrata da Bitdefender Total Security, Internet Security e Antivirus Plus ad agosto 2022 può essere eliminata selezionando il pulsante "x". La finestra "Gestisci le tue password con Bitdefender Password Manager" comparirà un paio di volte prima di scomparire del tutto. Puoi interrompere questo messaggio promozionale disattivando le **Notifiche di suggerimento** nelle Impostazioni di Bitdefender.

Cosa succede alla scadenza di Bitdefender Password Manager?

Una volta scaduto l'abbonamento a Password Manager, avrai un massimo di 90 giorni per esportare le tue password. Verrà eseguito il backup delle tue password per altri 30 giorni. Durante questi 90 giorni, potrai solo esportare i tuoi dati. Non potrai continuare a usare Password Manager. La funzionalità di compilazione automatica smetterà di funzionare, così come la possibilità di generare password.

Al termine del periodo di proroga di 90 giorni, avrai altri 30 giorni per contattare il supporto di Bitdefender e richiedere di ripristinare le tue password nel database live. Successivamente, potrai esportarle da Bitdefender Password Manager.

I tuoi dati saranno conservati nel database live solo fino alla fine del giorno in cui sono stati ripristinati su richiesta. Alla mezzanotte, il database sarà eliminato e, se non avrai ancora superato il periodo aggiuntivo di 30 giorni, le password potranno essere nuovamente ripristinate dal backup. I dati grezzi del database dal backup possono essere forniti su richiesta all'utente, ma il database è cifrato e le informazioni non sono accessibili.

Cos'è la password principale e perché devo ricordarmela?

La password principale è la chiave che apre la porta a tutte le password memorizzate nel tuo account di Bitdefender Password Manager. La password principale deve avere almeno 8 caratteri. Quindi crea una password principale sicura, memorizzala e non condividerla mai con nessuno. Per creare una password principale sicura, ti consigliamo di usare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

Come posso indicare a Bitdefender di non chiedermi più la mia password principale ogni volta che apro il browser?

Se blocchi il tuo dispositivo senza chiudere il browser, Password Manager non si chiuderà e potrai accedere ai tuoi dati quando tornerai. Come misura di sicurezza, ogni volta che apri il browser dovrai accedere al tuo account di Bitdefender Central e poi inserire la tua password principale.

- Per bloccare la richiesta di accesso di Central, vai in Impostazioni e seleziona "Disattiva la scheda di accesso all'avvio".
- Per bloccare la richiesta della password principale, seleziona la casella "Ricordami" nella schermata Sblocca il tuo vault.

Perché non memorizzate la mia password principale e cosa succede se me la dimentico?

Il motivo per cui non memorizziamo la tua password principale sui nostri server è per essere certi che solo tu possa accedere al tuo account. È il modo più sicuro. Se Bitdefender Password Manager non riconosce la tua password principale, assicurati di digitarla correttamente e che il tasto Blocca maiuscole non sia attivo sulla tastiera.

Se hai dimenticato la password principale, puoi sempre usare il codice di recupero per sbloccare Password Manager. Durante la fase di registrazione, Bitdefender Password Manager ti fornisce un {1}codice di recupero{2} che può essere usato per riottenere l'accesso al tuo account senza perdere i tuoi dati.

Se hai dimenticato o smarrito sia la password principale che il codice di recupero, come ultima possibilità, contatta un responsabile di Bitdefender per reimpostare il tuo account.

> **Importante**
> Reimpostare il tuo account eliminerà tutte le tue password e i tuoi dati salvati in Bitdefender Password Manager.

È possibile per più utenti condividere un abbonamento a Bitdefender Password Manager?

Per ora, non è possibile avere più utenti con lo stesso abbonamento di Password Manager, ma stiamo lavorando per attivare questa funzionalità in un prossimo futuro.

Cos'è la modalità offline e come funziona?

La modalità offline viene attivata automaticamente quando cade la connessione Internet mentre si usa Bitdefender Password Manager. Se hai già effettuato l'accesso e hai inserito la tua password principale, la modalità offline ti consente di accedere alle tue password quando non è possibile utilizzare una connessione a Internet.

Come disinstallo Bitdefender Password Manager?

Per disinstallare Bitdefender Password Manager:

- Su Windows e macOS:
  Rimuovi l'estensione di Password Manager dal tuo browser web. Clicca con il pulsante destro sull'icona di Bitdefender e seleziona "Rimuovi".
- Su Android:
  Tocca e tieni premuto la app Password Manager, poi trascinala nella parte superiore dello schermo dove dice "Disinstalla".
- Su iOS e iPadOS:
  Tocca e tieni premuto la app Password Manager finché tutte le app sul tuo schermo iniziano a vibrare, poi tocca la X nell'angolo in alto a sinistra dell'icona di Bitdefender.

Domande su privacy e sicurezza su Bitdefender Password Manager

I dipendenti di Bitdefender possono visualizzare le mie password?

Assolutamente no. La tua privacy è la nostra massima priorità. Questo è il motivo principale per cui non memorizziamo la tua password principale sui nostri server per i dati: in modo che nessuno abbia accesso al tuo account, nemmeno i dipendenti dell'azienda. Ogni password e account sono altamente cifrati con gli algoritmi di sicurezza dei dati più potenti e il codice che vediamo appare come una semplice stringa casuale di numeri e lettere mescolati tra loro.

Cosa succede se i server di Password Manager vengono violati?

Ogni password è cifrata a livello locale sul tuo dispositivo prima che si avvicini ai nostri server, così se degli hacker entrassero nel nostro sistema, riceverebbero solo pagine di lettere e numeri casuali senza il tuo codice per decifrarli. Ciò significa che sia tu che i dettagli del tuo account sarete sempre al sicuro con noi.

7. OTTENERE AIUTO

7.1. Richiesta d'aiuto

Bitdefender offre ai suoi clienti un livello impareggiabile di supporto rapido e accurato. Se dovessi riscontrare un qualche problema o se avessi domande sul tuo prodotto Bitdefender, potrai usare diverse risorse online per trovare una soluzione o una risposta. Allo stesso tempo, potrai contattare il servizio clienti di Bitdefender. I nostri responsabili del supporto risponderanno alle tue domande in maniera tempestiva e ti forniranno tutto l'aiuto necessario.

7.2. Risorse online

Sono disponibili diverse risorse online per aiutarti a risolvere i tuoi problemi e le tue domande relative a Bitdefender.

- Centro di supporto di Bitdefender:
  https://www.bitdefender.it/consumer/support/
- La community di esperti di Bitdefender:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Puoi anche usare il tuo motore di ricerca preferito per trovare più informazioni sulla sicurezza del computer, i prodotti Bitdefender e la società.

7.2.1. Centro di supporto di Bitdefender

Il Centro di supporto di Bitdefender è un archivio online di informazioni sui prodotti Bitdefender. Conserva, in un formato facilmente accessibile, le notifiche sui risultati delle attività di risoluzioni bug e problemi del supporto tecnico di Bitdefender e dei team di sviluppo, oltre ad articoli più generali sulla prevenzione delle minacce, la gestione delle soluzioni di Bitdefender con spiegazioni dettagliate e molti altri articoli.

Il Centro di supporto di Bitdefender è aperto al pubblico e gratuitamente esplorabile. Le ricche informazioni che contiene sono un altro modo per fornire ai clienti di Bitdefender le conoscenze tecnologiche e le

informazioni necessarie. Tutte le richieste di informazioni o i rapporti sui difetti, provenienti dai clienti di Bitdefender, prima o poi arrivano al Centro di supporto di Bitdefender, come rapporti di disinfezione, metodi per aggirare le truffe, o articoli informativi, per integrare i file di aiuto dei prodotti.

Il Centro assistenza di Bitdefender è disponibile in qualsiasi momento al seguente indirizzo: https://www.bitdefender.it/consumer/support/.

7.2.2. La community di esperti di Bitdefender

La community di esperti è un ambiente in cui gli utenti di Bitdefender, oltre a fan e appassionati, possono interagire, scambiare idee, supportarsi a vicenda e condividere le proprie conoscenze e soluzioni. È anche un luogo creativo e fornisce feedback preziosi ai nostri team di sviluppo. I membri della community sono utenti esperti di Bitdefender, felici di aiutare altri utenti nel proprio tempo libero. Grazie al loro immenso contributo e sforzi volontari, abbiamo creato una knowledge base dove gli utenti possono trovare risposte e aiuto, ma con un tocco più umano di una semplice risposta automatizzata.

Qui potrai trovare molte conversazioni utili con utenti che utilizzano Bitdefender sui propri dispositivi. La community offre una vera connessione con i nostri membri e fa sentire la loro voce. Ti invitiamo a parteciparvi sapendo che la tua opinione e le tue informazioni saranno rispettate e apprezzate. In qualità di fornitore stimato, ci sforziamo di offrire un livello senza precedenti di supporto sempre rapido e preciso, sperando di avvicinare sempre più i nostri utenti. Abbiamo progettato la nostra community con questo obiettivo sempre in mente.

Puoi trovare la pagina web della nostra community di esperti qui:

https://community.bitdefender.com/en/

7.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia include tutte le informazioni necessarie sulle minacce informatiche più recenti. È anche dove gli esperti Bitdefender condividono trucchi e suggerimenti su come restare protetti da hacker, violazioni, furti d'identità e tentativi d'impersonificazione dei social.

La pagina web di Bitdefender Cyberpedia è disponibile qui:

https://www.bitdefender.com/cyberpedia/.

7.3. Informazioni di contatto

Una comunicazione efficiente è la chiave per un business di successo. Dal 2001 BITDEFENDER ha stabilito una reputazione indiscutibile impegnandosi costantemente per una migliore comunicazione in modo da superare le aspettative dei nostri clienti e partner. In caso di domande, non esitate a contattarci direttamente tramite il ns Centro di supporto di Bitdefender (pagina 31).

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

7.3.1. Distributori locali

I distributori locali di Bitdefender sono pronti a rispondere a ogni richiesta inerente le loro zone operative, sia in ambito commerciale sia generale.

Per trovare un distributore di Bitdefender nel tuo paese:

1. Vai a https://www.bitdefender.com/partners/partner-locator.html.
2. Seleziona il tuo paese e la tua città, utilizzando le opzioni corrispondenti.

GLOSSARIO

Codice di attivazione

È una chiave univoca che può essere acquistata al dettaglio e utilizzata per attivare un prodotto o servizio specifico. Un codice di attivazione consente l'attivazione di un abbonamento valido per un certo periodo di tempo e numero di dispositivi e può essere utilizzato anche per estendere un abbonamento con la condizione da generare per lo stesso prodotto o servizio.

ActiveX

ActiveX è un modello per la scrittura di programmi in modo che altri programmi e il sistema operativo possano chiamarli. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per creare pagine Web interattive che sembrano e si comportano come programmi per computer, piuttosto che come pagine statiche. Con ActiveX, gli utenti possono porre o rispondere a domande, utilizzare pulsanti e interagire in altri modi con la pagina web. I controlli ActiveX vengono spesso scritti utilizzando Visual Basic. Active X si distingue per una completa mancanza di controlli di sicurezza; gli esperti di sicurezza informatica ne scoraggiano l'uso su Internet.

Minaccia persistente avanzata

Advanced Persistent Threat (APT) sfrutta le vulnerabilità dei sistemi per rubare informazioni importanti per consegnarle alla fonte. Grandi gruppi come organizzazioni, aziende o governi sono presi di mira da questa minaccia. L'obiettivo di una minaccia persistente avanzata è rimanere inosservato per lungo tempo essendo in grado di monitorare e raccogliere informazioni importanti senza danneggiare le macchine mirate. Il metodo utilizzato per iniettare la minaccia nella rete è attraverso un file PDF o un documento di Office che sembra innocuo in modo che ogni utente possa eseguire i file.

Adware

L'adware è spesso combinato con un'app host fornita gratuitamente a condizione che l'utente accetti l'adware. Poiché le app adware vengono generalmente installate dopo che l'utente ha accettato un contratto di licenza che stabilisce lo scopo dell'app, non viene commesso alcun reato. Tuttavia, le pubblicità pop-up possono diventare fastidiose e in alcuni casi

degradare le prestazioni del sistema. Inoltre, le informazioni raccolte da alcune di queste app possono causare problemi di privacy per gli utenti che non erano pienamente a conoscenza dei termini del contratto di licenza.

Archivio

Un disco, un nastro o una cartella che contiene file memorizzati.

Un file che contiene uno o più file in un formato compresso.

Porta sul retro

Un buco nella sicurezza di un sistema deliberatamente lasciato in essere da progettisti o manutentori. La motivazione di tali buchi non è sempre sinistra; alcuni sistemi operativi, ad esempio, escono dalla confezione con account privilegiati destinati all'uso da parte dei tecnici dell'assistenza sul campo o dei programmatori di manutenzione del fornitore.

Settore di avvio

Un settore all'inizio di ogni disco che identifica l'architettura del disco (dimensione del settore, dimensione del cluster e così via). Per i dischi di avvio, il settore di avvio contiene anche un programma che carica il sistema operativo.

Avvio virus

Una minaccia che infetta il settore di avvio di un disco fisso o floppy. Un tentativo di avvio da un dischetto infettato da un virus del settore di avvio causerà l'attivazione della minaccia nella memoria. Ogni volta che avvierai il tuo sistema da quel momento in poi, avrai la minaccia attiva in memoria.

Botnet

Il termine “botnet” è composto dalle parole “robot” e “network”. Le botnet sono dispositivi connessi a Internet infettati da minacce e possono essere utilizzati per inviare e-mail di spam, rubare dati, controllare da remoto dispositivi vulnerabili o diffondere spyware, ransomware e altri tipi di minacce. Il loro obiettivo è quello di infettare il maggior numero possibile di dispositivi connessi, come PC, server, dispositivi mobili o IoT appartenenti a grandi aziende o industrie.

Navigatore

Abbreviazione di browser Web, un'app software utilizzata per individuare e visualizzare pagine Web. I browser più diffusi includono Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Questi sono browser

grafici, il che significa che possono visualizzare grafica e testo. Inoltre, la maggior parte dei browser moderni può presentare informazioni multimediali, inclusi audio e video, sebbene richiedano plug-in per alcuni formati.

Attacco di forza bruta

Attacco di indovinazione della password utilizzato per irrompere in un sistema informatico inserendo possibili combinazioni di password, per lo più a partire dalla password più facile da indovinare.

Riga di comando

In un'interfaccia a riga di comando, l'utente digita i comandi nello spazio fornito direttamente sullo schermo utilizzando il linguaggio dei comandi.

Biscotti

Nell'industria di Internet, i cookie sono descritti come piccoli file contenenti informazioni su singoli computer che possono essere analizzati e utilizzati dagli inserzionisti per tenere traccia dei tuoi interessi e gusti online. In questo ambito, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di indirizzare gli annunci direttamente a ciò che hai dichiarato di essere i tuoi interessi. È un'arma a doppio taglio per molte persone perché, da un lato, è efficiente e pertinente in quanto si vedono solo annunci su ciò che ti interessa. cosa clicchi. Comprensibilmente, c'è un dibattito sulla privacy e molte persone si sentono offese dall'idea di essere viste come un "numero SKU" (sai, il codice a barre sul retro dei pacchi che viene scansionato alla cassa della drogheria) . Sebbene questo punto di vista possa essere estremo, in alcuni casi è accurato.

Cyber bullismo

Quando coetanei o estranei commettono atti violenti contro i bambini apposta per ferirli fisicamente. Per danneggiare emotivamente, gli aggressori inviano messaggi meschini o foto poco lusinghiere, isolando così le loro vittime dagli altri o sentendosi frustrate.

Dizionario Attacco

Attacchi di indovinazione della password utilizzati per irrompere in un sistema informatico inserendo una combinazione di parole comuni per generare potenziali password. Lo stesso metodo viene utilizzato per indovinare le chiavi di decrittazione di messaggi o documenti crittografati.

Gli attacchi con dizionario hanno successo perché molte persone tendono a scegliere password brevi e con parole singole facili da indovinare.

Unità disco

È una macchina che legge e scrive dati su un disco. Un disco rigido legge e scrive dischi rigidi. Un'unità floppy accede ai dischi floppy. Le unità disco possono essere interne (alloggiate all'interno di un computer) o esterne (alloggiate in una scatola separata che si collega al computer).

Scaricamento

Per copiare i dati (di solito un intero file) da una fonte principale a un dispositivo periferico. Il termine è spesso usato per descrivere il processo di copia di un file da un servizio online al proprio computer. Il download può anche riferirsi alla copia di un file da un file server di rete a un computer in rete.

E-mail

Mail elettronica. Un servizio che invia messaggi sui computer tramite reti locali o globali.

Eventi

Un'azione o un evento rilevato da un programma. Gli eventi possono essere azioni dell'utente, come fare clic su un pulsante del mouse o premere un tasto, o occorrenze di sistema, come l'esaurimento della memoria.

Exploit

Un modo per sfruttare diversi bug o vulnerabilità presenti in un computer (software o hardware). Pertanto, gli hacker possono ottenere il controllo di computer o reti.

Falso positivo

Si verifica quando uno scanner identifica un file come infetto quando in realtà non lo è.

Estensione del nome file

La parte di un nome di file, dopo il punto finale, che indica il tipo di dati memorizzati nel file. Molti sistemi operativi utilizzano estensioni di file, ad esempio Unix, VMS e MS-DOS. Di solito sono da una a tre lettere (alcuni tristi vecchi sistemi operativi non supportano più di tre). Gli esempi includono "c" per codice sorgente C, "ps" per PostScript, "txt" per testo arbitrario.

Euristico

Un metodo basato su regole per identificare nuove minacce. Questo metodo di scansione non si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione euristica è che non viene ingannata da una nuova variante di una minaccia esistente. Tuttavia, potrebbe occasionalmente segnalare codice sospetto nei normali programmi, generando il cosiddetto "falso positivo".

Vaso di miele

Un sistema informatico esca impostato per attirare gli hacker per studiare il modo in cui agiscono e identificare i metodi eretici che utilizzano per raccogliere informazioni di sistema. Le aziende e le aziende sono più interessate a implementare e utilizzare gli honeypot per migliorare il proprio stato di sicurezza generale.

IP

Protocollo Internet - Un protocollo instradabile nella suite di protocolli TCP/IP responsabile dell'indirizzamento IP, del routing e della frammentazione e riassemblaggio dei pacchetti IP.

Applet Java

Un programma Java progettato per essere eseguito solo su una pagina Web. Per utilizzare un'applet su una pagina Web, devi specificare il nome dell'applet e la dimensione (lunghezza e larghezza, in pixel) che l'applet può utilizzare. Quando si accede alla pagina Web, il browser scarica l'applet da un server e la esegue sulla macchina dell'utente (il client). Le applet differiscono dalle app in quanto sono governate da un rigido protocollo di sicurezza.

Ad esempio, anche se le applet vengono eseguite sul client, non possono leggere o scrivere dati sulla macchina del client. Inoltre, le applet sono ulteriormente limitate in modo che possano solo leggere e scrivere dati dallo stesso dominio da cui sono servite.

Registratore di tasti

Un keylogger è un'app che registra tutto ciò che digiti. I keylogger non sono di natura dannosa. Possono essere utilizzati per scopi legittimi, come il monitoraggio dell'attività dei dipendenti o dei bambini. Tuttavia, vengono sempre più utilizzati dai criminali informatici per scopi dannosi (ad esempio, per raccogliere dati privati, come credenziali di accesso e numeri di previdenza sociale).

Virus a macroistruzione

Un tipo di minaccia informatica codificata come macro incorporata in un documento. Molte app, come Microsoft Word ed Excel, supportano potenti linguaggi macro. Queste app ti consentono di incorporare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Cliente di posta

Un client di posta elettronica è un'app che consente di inviare e ricevere e-mail.

Memoria

Aree di archiviazione interne nel computer. Il termine memoria identifica l'archiviazione dei dati sotto forma di chip e la parola archiviazione viene utilizzata per la memoria che esiste su nastri o dischi. Ogni computer viene fornito con una certa quantità di memoria fisica, solitamente indicata come memoria principale o RAM.

Non euristico

Questo metodo di scansione si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione non euristica è che non si lascia ingannare da quella che potrebbe sembrare una minaccia e non genera falsi allarmi.

Predatori online

Individui che cercano di attirare minori o adolescenti in conversazioni apposta per coinvolgerli in attività sessuali illegali. I social network sono il luogo ideale in cui i bambini vulnerabili possono essere facilmente cacciati e indotti a commettere attività sessuali, online o faccia a faccia.

Programmi confezionati

Un file in un formato di compressione. Molti sistemi operativi e app contengono comandi che consentono di comprimere un file in modo che occupi meno memoria. Ad esempio, supponi di avere un file di testo contenente dieci caratteri spazio consecutivi. Normalmente, ciò richiederebbe dieci byte di archiviazione.

Tuttavia, un programma che comprime i file sostituirà i caratteri di spazio con uno speciale carattere di serie di spazi seguito dal numero di spazi da sostituire. In questo caso, i dieci spazi richiederebbero solo due byte. Questa è solo una delle tecniche di confezionamento, ce ne sono molte altre.

Sentiero

Le indicazioni esatte per un file su un computer. Queste direzioni sono solitamente descritte per mezzo del sistema di archiviazione gerarchico dall'alto verso il basso.

Il percorso tra due punti qualsiasi, ad esempio il canale di comunicazione tra due computer.

Phishing

L'atto di inviare un'e-mail a un utente che afferma falsamente di essere un'impresa legittima e consolidata nel tentativo di indurre l'utente a cedere informazioni private che verranno utilizzate per il furto di identità. L'e-mail indirizza l'utente a visitare un sito Web in cui viene chiesto di aggiornare le informazioni personali, come password e numeri di carta di credito, previdenza sociale e conto bancario, che l'organizzazione legittima già possiede. Il sito Web, tuttavia, è fasullo e impostato solo per rubare le informazioni dell'utente.

Fotone

Photon è una tecnologia di Bitdefender innovativa e discreta, progettata per minimizzare l'impatto della tua soluzione di sicurezza sulle prestazioni del sistema. Monitorando in background l'attività del PC, crea degli schemi di utilizzo, per ottimizzare i processi di avvio e scansione.

Virus polimorfo

Una minaccia che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, queste minacce sono difficili da identificare.

Porta

Un'interfaccia su un computer alla quale puoi connettere un supporto. I PC hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta identifica di che tipo di porta si tratta. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Ransomware

Un ransomware è un programma dannoso che prova a sottrarre illecitamente denaro agli utenti bloccando i loro sistemi vulnerabili.

CryptoLocker, CryptoWall e TeslaWall sono solo alcune delle varianti che cercano di bloccare i sistemi personali degli utenti.

L'infezione può partire, aprendo e-mail di spam, scaricando gli allegati di un messaggio o installando determinate applicazioni, il tutto lasciando l'utente ignaro di ciò che sta accadendo sul suo sistema. Gli autori di ransomware puntano a colpire soprattutto gli utenti normali e le aziende.

File di rapporto

File che elenca le azioni avvenute. Bitdefender mantiene un file di rapporto che elenca i percorsi esaminati, le cartelle, il numero di archivi e i file esaminati, oltre a quanti file infetti e sospetti sono stati trovati.

Rootkit

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore a un sistema. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza in modo da non dover essere visti dai veri amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere minacce o per celare la presenza di un intruso nel sistema. Se combinati alle minacce, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuti come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessione a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un Trojan che gli utenti installano inconsapevolmente installando altre applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

Articoli di avvio

Qualsiasi file posizionato in questa cartella si aprirà all'avvio del computer. Ad esempio, una schermata di avvio, un file audio da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure app che possono essere elementi di avvio. Normalmente in questa cartella viene posizionato un alias di un file, al posto del file stesso.

Abbonamento

Un accordo di acquisto che offre all'utente il diritto di utilizzare un particolare prodotto o servizio su un numero specifico di dispositivi e per un certo periodo di tempo. Un abbonamento scaduto può essere rinnovato automaticamente, utilizzando le informazioni fornite dall'utente con il primo acquisto.

Area di notifica

Introdotta con Windows 95, la barra degli strumenti è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o

clicca con il pulsante destro su un'icona per visualizzare e accedere a dettagli e controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

Minaccia

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte delle minacce è anche in grado di auto replicarsi. Tutte le minacce informatiche sono state create dall'uomo. È relativamente facile produrre una semplice minaccia in grado di copiare sé stessa innumerevoli volte. Persino una minaccia così semplice è pericolosa in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di minaccia ancora più pericolosa è quella in grado di trasmettere sé stessa attraverso le reti superando i sistemi di sicurezza.

Aggiornamento delle informazioni sulle minacce

Lo schema binario di una minaccia, usato dalla soluzione di sicurezza per rilevare ed eliminare la minaccia.

Troiano

Un programma distruttivo che si maschera da applicazione benevola. A differenza di programmi software dannosi e worm, i trojan non si replicano ma possono essere altrettanto distruttivi. Un tipo di minaccia Trojan particolarmente insidiosa è un programma che dichiara di pulire le minacce dal computer, ma al contrario le introduce.

Il termine deriva dalla storia dell'Iliade di Omero, dove i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, durante la notte, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire una versione precedente dello stesso prodotto. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul computer; diversamente non sarà possibile installare l'aggiornamento.

Bitdefender dispone della propria funzionalità di aggiornamento, che consente la verifica manuale degli aggiornamenti, oppure l'aggiornamento automatico del prodotto.

Rete privata virtuale (VPN)

È una tecnologia che consente una connessione diretta temporanea e cifrata a una determinata rete su una rete meno sicura. In questo modo, la ricezione e l'invio dei dati sono sempre sicuri e cifrati, ma soprattutto più difficili da intercettare dai pirati informatici. Una prova di sicurezza è l'autenticazione, che può essere fatta solo usando un nome utente e una password.

Verme

Programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.