MANUALE D'USO

Bitdefender CONSUMER SOLUTIONS

# SecurePass

# Bitdefender SecurePass

**Guida dell'utente**

Publication date 20/11/2024


## Avviso legale



Bitdefender

# Indice

# INFORMAZIONI SU QUESTA GUIDA

## Finalità e destinatari

Questo manuale è rivolto a tutti gli utenti Bitdefender che hanno scelto Bitdefender SecurePass 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 SecurePass e il processo di installazione.

Importare ed esportare le tue password (pagina 10)

Scopri come importare o esportare le password in entrata e in uscita da SecurePass.

Caratteristiche e funzionalità (pagina 14)

Scopri come usare Bitdefender SecurePass e tutte le sue funzionalità.

Ottenere aiuto (pagina 27)

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 SECUREPASS

Bitdefender SecurePass 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 SecurePass 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. 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 SecurePass solo su dispositivi con i seguenti sistemi operativi:

- **Per gli utenti PC:**
  - Windows 7 con Service Pack 1
  - 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 SecurePass 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 SecurePass o il prodotto potrebbe non funzionare correttamente.

## 2.2. Installazione

Questo capitolo ti illustrerà come installare Bitdefender SecurePass 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**.

- **Google Chrome**
- **Mozilla Firefox**
- **Microsoft Edge**
- **Safari**

Per installare Bitdefender SecurePass:

1. Dopo aver acquistato Bitdefender SecurePass, segui i passaggi forniti nell'e-mail di conferma per attivare l'abbonamento.
2. Accedi a Bitdefender Central utilizzando le tue credenziali.
   Nel menu a sinistra, seleziona **SecurePass**.
3. Nel pannello SecurePass, seleziona il tuo browser preferito.
4. Installa l'estensione del browser:
   - **Google Chrome:**
     a. Fai clic su **Aggiungi a Chrome** pulsante
     b. Nella casella di conferma, fai clic su **Aggiungi estensione**.
   - **Mozilla Firefox:**
     a. Fai clic su **Aggiungi a Firefox** pulsante.
     b. Fai clic su **Installa** pulsante nell'angolo in alto a destra dello schermo.
   - **Microsoft Edge:**
     a. Fai clic su **Ottieni** pulsante.
     b. Fare clic **Aggiungi estensione** nel prompt che appare.
   - **Safari:**
     a. Il programma di installazione di SecurePass verrà scaricato sul tuo dispositivo macOS. Fai doppio clic sul file scaricato e segui le
     b. Al termine del processo di installazione, apri **Safari** browser e seleziona **Preferenze** nella barra dei menu in alto.
     c. Nella finestra Preferenze, fai clic su **scheda Estensioni**.

d. Seleziona la casella accanto a **Bitdefender SecurePass** per abilitarlo.

Una volta installata l'estensione, puoi procedere al Processo di installazione (pagina 9).

### 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.

1. Prima di tutto, dopo l'acquisto, assicuratevi di aprire l'e-mail di conferma ricevuta per seguire le istruzioni ivi fornite per attivare l'abbonamento SecurePass.
2. Apri Google Play Store sul tuo dispositivo Android.
3. Nella barra di ricerca del Google Play Store, digita **Bitdefender SecurePass**, individua e scarica l'applicazione.
4. Una volta completato il download, apri l'app e, se necessario, segui i passaggi di configurazione sullo schermo necessari per completare il processo di installazione.

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.

1. Prima di tutto, dopo l'acquisto, assicuratevi di aprire l'e-mail di conferma ricevuta per seguire le istruzioni ivi fornite per attivare l'abbonamento SecurePass.
2. Apri l'App Store sul tuo dispositivo iOS.
3. Nella barra di ricerca dell'App Store, digita **Bitdefender SecurePass**, individua e scarica l'applicazione.
4. Una volta completato il download, apri l'app e, se necessario, segui i passaggi di configurazione sullo schermo necessari per completare il processo di installazione.

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

## 2.3. Processo di installazione

Per configurare Bitdefender SecurePass sul tuo browser/dispositivo mobile:

1. Dopo aver terminato il processo di installazione, apri l'estensione/applicazione SecurePass ed effettua il login.
   Usa le credenziali dell'account Bitdefender associato al tuo abbonamento SecurePass.
2. Ti verrà richiesto di creare un **Password principale**.

   > **Importante**
   > Tieni presente che avrai bisogno di questa password principale per sbloccare tutte le password, i dati della carta di credito e le note salvate in Bitdefender SecurePass. Questa è essenzialmente la chiave che consente al proprietario di utilizzare

   Assicurati di inserire una password principale sicura senza il rischio di dimenticarla facilmente.
   Una volta scelta una password principale sicura e unica, fai clic su **Salva e continua**.
3. Successivamente, ti verrà fornito un **Chiave di ripristino**.

   > **Avvertenza**
   > Dopo aver creato la Master Password, riceverai una **Chiave di ripristino a 24 cifre**. Annota la tua chiave di ripristino in un posto sicuro e non perderla. Questa chiave è l'unico modo per accedere alle password salvate in Password Manager nel caso in cui vi capiti **dimentica la password principale** precedentemente configurato per il tuo account.
   >
   > - Salva la chiave di ripristino copiandola negli appunti o scaricandola come file PDF.
   >   Puoi premere **Chiudi** quando è finito.
4. Una volta fatto, seleziona **Accedi al tuo Vault** pulsante.

Ora che il processo di configurazione è completo, puoi iniziare a utilizzare Bitdefender SecurePass.

# 3. 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.

## 3.1. Compatibilità

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

- Gestore di password Bitdefender
- Portafoglio Bitdefender
- Bitdefender SecurePass
- SaferPass
- 1 password
- Kaspersky
- Dashlane
- Browser Chrome
- Browser Firefox
- Microsoft Edge
- Bitwarden
- LastPass
- Mantieni Pass
- RoboForm

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**.

## 3.2. 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. Apri Bitdefender SecurePass e vai su **Impostazioni**.
   - Nel browser:
     Clicca su **Impostazioni** nell'angolo in alto a destra della pagina.
   - Nell'app:
     Tocca il **Altro** pulsante nell'angolo in basso a destra dello schermo e, nella parte superiore dell'elenco che appare dopo, tocca **Impostazioni**.
2. Nel **Backup e ripristino** sezione, seleziona **Importa password**. Si aprirà la finestra di importazione.
3. Seleziona il nome del gestore di password o del browser web che hai utilizzato in precedenza dal menu a discesa accessibile tramite **Seleziona il tipo di file** campo.

   > **Nota**
   > Se è stata utilizzata una password per crittografare il file, ti verrà richiesto di inserirla nel **Password** campo; in caso contrario, puoi lasciarlo vuoto.

4. Seleziona il **Seleziona il file da importare** archiviato.
   Vai alla posizione in cui sono stati salvati i dati esportati appartenenti al tuo vecchio gestore di password. Scegli il file una volta trovato, quindi fai clic su **Apri**.

5. Dopo aver selezionato il file, seleziona **Importa** nell'angolo inferiore sinistro della finestra di importazione. Il processo inizierà a breve, accompagnato da una barra di avanzamento

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.

> **Nota**
> Tornando all'archivio delle password in SecurePass, noterai una cartella denominata **Importa**, contenente tutti i dati del tuo precedente gestore di password o browser web.

## 3.3. 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. Apri Bitdefender SecurePass e vai su **Impostazioni**.
   - Nel browser:
     Clicca su **Impostazioni** nell'angolo in alto a destra della pagina.
   - Nell'app:
     Tocca il **Altro** pulsante nell'angolo in basso a destra dello schermo e, nella parte superiore dell'elenco che appare dopo, tocca **Impostazioni**.
2. Nel **Backup e ripristino** sezione, seleziona **Esporta le password**. Si aprirà la finestra di esportazione.

3. Clicca su **Seleziona il tipo di file**. Dal menu a discesa, scegli di esportare i tuoi dati in formato JSON o CSV. Puoi anche inserire una password con cui proteggere il file esportato
   Seleziona la casella corrispondente se desideri includere anche elementi condivisi.
4. Fare clic **Esporta** nell'angolo inferiore sinistro della finestra di esportazione e salva il file esportato sul tuo dispositivo.

# 4. 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.

## 4.1. Salvare manualmente le password

Puoi archiviare in modo sicuro informazioni come password, credenziali e altro, come i dati della carta di credito o le note in Bitdefender SecurePass manualmente, nel modo seguente:

1. Apri Bitdefender SecurePass
2. Nel **Il mio caveau** scheda, premi il **+Aggiungi articolo** pulsante.
3. Seleziona il tipo di articolo che desideri aggiungere. (conto, carta di credito, identità o nota).
4. Compila i campi obbligatori in base all'articolo selezionato.
5. Dopo aver completato tutti i dettagli necessari, salva l'articolo per aggiungerlo al tuo vault SecurePass.

## 4.2. Generatore di password

Bitdefender SecurePass include una funzione di generazione di password che può aiutare nella creazione di password sicure.

Per accedere e utilizzare il generatore di password:

1. Apri Bitdefender SecurePass e accedi al **Genera la password** scheda sul lato sinistro dello schermo. Verrai reindirizzato al generatore di password integrato in SecurePass
2. Personalizza la password che stai per generare in base alle tue esigenze e preferenze.
   - Lunghezza della password: trascina il cursore per determinare una lunghezza compresa tra 8 e 32 caratteri.
   - Lettere maiuscole/minuscole: seleziona quali o entrambi i tipi di lettere desideri aggiungere per il livello di complessità della tua password.

- Numeri: selezionando questa casella verranno inclusi i numeri nella stringa di caratteri che compone la password.
- Caratteri speciali: aggiungi simboli alla tua password per aumentarne la complessità.

> **Nota**
> Premere il **Salva le impostazioni** pulsante per consentire a SecurePass di ricordarle e generare sempre le password in base alle impostazioni salvate.

3. Genera una nuova password facendo clic sull'icona a forma di freccia circolare situata sotto la password attualmente visualizzata. Ogni clic genera una nuova stringa di caratteri
4. Una volta soddisfatto della password generata, puoi copiarla negli appunti o fare clic su **Salva l'account** pulsante per salvarlo nel tuo vault (associandolo ad altre informazioni sull'account).

> **Nota**
> Puoi anche generare rapidamente una password **direttamente dai moduli di iscrizione** facendo clic sull'icona Bitdefender SecurePass presente nel campo della password della pagina di registrazione. Cliccando su di essa, puoi quindi scegliere **Genera la password** opzione

## 4.3. Controllo della sicurezza della password

Bitdefender SecurePass offre la possibilità di valutare la sicurezza delle password salvate e dei dati sensibili. Questa è una funzionalità fondamentale per valutare e valutare eventuali vulnerabilità alla privacy e alla

Per verificare i punti di forza delle password memorizzate:

1. Apri Bitdefender SecurePass e, nel menu della posta, seleziona **Rapporto di sicurezza** scheda.
   La scheda Rapporto sulla sicurezza è suddivisa in quattro sezioni: violato, debole, vecchio e duplicato.
2. Il numero di password che rientrano in ciascuna delle quattro categorie verrà visualizzato sullo schermo.

Inoltre, scorrendo l'elenco delle password memorizzate, ciascuna password verrà contrassegnata con la categoria in cui si trova.

Per comprendere il significato di questi livelli di sicurezza, di seguito sono riportati alcuni brevi dettagli su ciascuno di essi:

- Password violate: se una delle tue credenziali è stata oggetto di una violazione dei dati, verrà elencata nella **violato** sezione.

  > **Nota**
  > Per verificare se una delle tue password è stata compromessa e divulgata a causa di violazioni dei dati, fai clic su **Esegui una scansione di sicurezza** pulsante.

- Password deboli: SecurePass identificherà e contrassegnerà **deboli** password archiviate nel vault sulla base di un algoritmo interno, eseguito localmente, che analizza vari criteri, tra cui la lunghezza della password, la varietà di caratteri e l'inclusione di cifre o lettere maiuscole, tra gli altri fattori.
- Password precedenti: le password che sono state salvate e non modificate per un periodo superiore a sei mesi verranno contrassegnate come **vecchie**.
- Password duplicate: considerando che l'utilizzo delle stesse password su più piattaforme e account presenta un grosso rischio per la sicurezza, SecurePass contrassegnerà le password utilizzate in più di un posto come **duplicato**.

## 4.4. Organizzazione dei dati

All'interno di Bitdefender SecurePass, puoi organizzare e quindi gestire più facilmente tutti i tuoi elementi salvati.

Puoi classificare i tuoi elementi in cartelle specifiche per accedervi facilmente seguendo questi passaggi:

1. Apri Bitdefender SecurePass e vai su **La mia cassaforte**. Qui, tocca **Aggiungi cartella** pulsante
2. Assegna un nome alla cartella e tocca **Crea** pulsante.
   La nuova cartella verrà ora visualizzata nel tuo vault.

Per spostare gli elementi nella cartella creata:

1. Fai clic su qualsiasi account che desideri spostare e premi il pulsante **Modifica** pulsante.
2. Premi la posizione mostrata accanto a **Salva l'articolo in** e seleziona il nome della cartella dall'elenco a discesa.
3. Premere il **Salva account** pulsante.

L'account verrà ora archiviato nella cartella selezionata.

## 4.5. Riempimento automatico intelligente

Bitdefender SecurePass ti consente di compilare automaticamente le credenziali e le informazioni dell'account su qualsiasi modulo di accesso online.

> **Nota**
> Come estensione del browser Web, su Windows o macOS, la funzione di compilazione automatica dovrebbe funzionare senza problemi.

### 4.5.1. Riempimento automatico su Android

Per configurare SecurePass su Android per utilizzare la compilazione automatica:

1. Apri l'app Bitdefender SecurePass sul tuo dispositivo Android.
2. Tocca il **Altro** pulsante menu.
3. Nella parte superiore dello schermo, tocca **Impostazioni**.
4. Tocca **Imposta questo gestore di password predefinito**
5. Abilita Bitdefender SecurePass nell'elenco dei servizi di compilazione automatica.

   > **Nota**
   > Puoi anche accedere alle impostazioni del tuo dispositivo Android, in **Password e account** > **Servizio di compilazione automatica** > abilita Bitdefender SecurePass.
   >
   > Per Android 11 o versioni precedenti del sistema operativo, le impostazioni sono: **Sistema** > **Lingua e input** > **Avanzato**.

6. Tocca **OK**.

Una volta completata questa configurazione, ogni volta che tocchi un campo di accesso, sullo schermo apparirà un'opzione chiamata

Bitdefender SecurePass. Puoi toccarlo per aprire l'app. Accedi a SecurePass e le tue credenziali verranno inserite automaticamente

### 4.5.2. Compilazione automatica su iOS

Per configurare SecurePass sul tuo dispositivo iOS per utilizzare la compilazione automatica:

1. Aprire il **Impostazione** app sul tuo iPhone o iPad e seleziona **Generale**.
2. Tocca **Compilazione automatica e password**. Garantire l'opzione **Compilazione automatica di password e passkey** o **Compilazione automatica delle password** - a seconda della versione iOS - è attivata.
3. Nel **Modulo di compilazione automatica** elenco, abilita il **Bitdefender SecurePass** applicazione.

Una volta completata questa configurazione, ogni volta che tocchi un campo di accesso, sullo schermo apparirà un'opzione chiamata Bitdefender SecurePass. Puoi toccarlo per aprire l'app. Accedi a SecurePass e le tue credenziali verranno inserite automaticamente

### 4.5.3. Compilazione automatica dei dati della carta

Mentre SecurePass fornisce un'icona facilmente accessibile per la compilazione automatica delle credenziali di accesso e delle password, la funzione di compilazione automatica per i dati della carta di credito funziona in modo diverso:

1. Vai alla pagina di pagamento o pagamento del sito Web su cui desideri utilizzare i dati della tua carta di credito memorizzati.
2. Fai clic con il pulsante destro del mouse su un'area vuota della pagina di pagamento. Ciò richiederà la visualizzazione del menu contestuale sullo schermo
3. Seleziona Bitdefender SecurePass dal menu posizionando il cursore sull'opzione. Si aprirà
4. Scegli il **Compilazione automatica dei dati della carta di credito**. Verrà visualizzato un elenco di tutte le carte di credito archiviate nel vault di SecurePass
5. Seleziona la carta preferita.

In questo modo, SecurePass compilerà automaticamente i campi del modulo di pagamento con i dati della carta di credito scelta.

# 5. USA COME APPLICAZIONE 2FA

Puoi sempre scegliere di utilizzare Bitdefender SecurePass come app di autenticazione a due fattori per qualsiasi sito Web o piattaforma desideri e gestire i tuoi codici 2FA insieme alle tue password nel modo seguente:

1. Vai alle impostazioni di sicurezza del sito Web o dell'applicazione in cui desideri abilitare la funzione 2FA. In genere, durante il processo ti verrà presentato un codice QR o un codice di verifica
2. Avvia Bitdefender SecurePass e accedi all'account corrispondente che desideri configurare per l'uso della 2FA. **Modifica** pulsante.
3. Scorri fino alla fine della pagina di immissione dell'account in SecurePass e premi su **Autenticazione a due fattori** opzione
4. Scansiona il codice QR o inserisci il codice manualmente.
   Fatto ciò, SecurePass confermerà l'avvenuta configurazione dell'autenticazione a due fattori.
5. Dopodiché, premi il nuovo **Visualizza il codice** pulsante ora visibile nell'interfaccia. Qui viene visualizzato un codice sensibile al fattore tempo
6. Torna all'account in cui hai abilitato la funzione 2FA e inserisci il codice di Bitdefender SecurePass per verificare la tua configurazione.

Dopo aver completato questa procedura di configurazione, premere il pulsante **Salva account** pulsante in SecurePass per finalizzare il processo.

D'ora in poi, quando accedi alla piattaforma per la quale hai impostato la funzione 2FA, ti verrà richiesto di utilizzare i codici 2FA di SecurePass per il rispettivo account, offrendo un nuovo livello di sicurezza per l'account in questione.

# 6. CONDIVIDI DATI

Bitdefender SecurePass offre la possibilità di condividere informazioni sensibili in modo sicuro, come credenziali, password o dettagli della carta di credito.

È possibile utilizzare la funzione di condivisione tramite link:

1. Scegli un oggetto archiviato nel tuo vault.
   - Nel browser:
     Vai al tuo vault e fai clic sull'elemento che desideri condividere. Sul lato destro, fai clic sul menu a tre punti e **Condividi link**.
   - Nell'app:
     Vai al tuo vault e tocca l'elemento che desideri condividere. Tocca l'icona del link e scegli **Genera link di condivisione** opzione.
2. Crea il link Condividi specificando:
   - La data di scadenza del link.
   - Il limite di utilizzo.
   - Indica se il link deve essere protetto da password o meno.
3. Una volta generato, copia il link generato e invialo al destinatario previsto.

## 6.1. Condividi con i gruppi

I gruppi vengono creati allo scopo di rendere ancora più semplice la condivisione dei dati. Puoi creare vari gruppi all'interno di Bitdefender SecurePass con altri utenti per condividere in modo sicuro dati sensibili

1. Crea un gruppo:
   - Vai a **Gruppi** e premere il pulsante **Crea gruppo** pulsante nella scheda Gruppi.
   - Imposta un nome per il gruppo e premi il pulsante **Crea gruppo** pulsante.
2. Aggiungi elementi ai gruppi:
   - Nel browser:

Vai al tuo vault e fai clic sull'elemento che desideri condividere. Fai clic sul menu a tre punti sul lato destro dell'elemento e scegli **Aggiungi al gruppo**.

- Nell'app:
  Vai al tuo vault e fai clic sull'elemento che desideri condividere. Scegli il **Condividi con il gruppo** opzione

Seleziona il gruppo con cui desideri condividere l'articolo.

3. Imposta i diritti di accesso (lettura, scrittura, concessione) in base al livello di controllo che desideri fornire ai membri del gruppo.
4. Premere **Salva**, allora **Fatto**.

Tu e i membri del gruppo potete esaminare gli elementi condivisi nella sezione del gruppo.

## 6.2. Gestisci gruppi

Nel **Gruppi** nella sezione di Bitdefender SecurePass puoi esaminare tutti i gruppi creati e gestirli in base alle tue esigenze:

- Rinomina i gruppi.
- Modifica membri. (invitare nuovi membri, assegnare diritti a membri specifici, concedere diritti di amministratore o di condivisione e rimuovere membri esistenti)
- Abbandona i gruppi.
- Eliminare i gruppi.

# 7. BLOCCA ACCOUNT

Bitdefender SecurePass è dotato di **Blocca account** funzione che blocca istantaneamente il tuo account e termina tutte le sessioni attive su tutti i dispositivi che vi hanno accesso. Questa funzione è particolarmente utile quando sorgono sospetti di accesso non

Per bloccare il tuo account SecurePass:

1. Apri Bitdefender SecurePass.
2. Una volta in SecurePass:
   - Nel browser:
     Clicca su **Impostazioni** nell'angolo in alto a destra della pagina.
   - Nell'app mobile:
     Tocca il **Mettimi al sicuro** pulsante del menu.
3. Premere il **Blocca account** pulsante per disconnettersi istantaneamente da tutti i dispositivi e terminare le sessioni in corso.

# 8. 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

**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 @).

**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.

**Cos'è la modalità offline?**

La modalità offline si attiva automaticamente quando la connessione Internet si interrompe durante l'utilizzo di Bitdefender SecurePass. Se hai già effettuato l'accesso e hai inserito la tua password principale, la modalità Offline ti consente di accedere alle tue password quando una connessione Internet non è raggiungibile

**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.

# 9. OTTENERE AIUTO

## 9.1. 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.

## 9.2. 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.

### 9.2.1. 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/.

### 9.2.2. 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/

### 9.2.3. 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/.

## 9.3. 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 27).

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

### 9.3.1. 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 unica che può essere acquistata dal rivenditore e usata per attivare un servizio o un prodotto specifico. Un codice di attivazione consente l'attivazione di un abbonamento valido per un determinato periodo di tempo e un certo numero di dispositivi. Inoltre, può anche essere utilizzato per estendere un abbonamento, a condizione che venga generato 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.

**Virtual Private Network (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.