Bitdefender®
MOBILE SECURITY FOR iOS

MANUALE D'USO

iOS

Bitdefender Mobile Security for iOS

Guida dell'utente

Data di pubblicazione 22/11/2022

Avviso legale

Bitdefender

Indice

Informazioni su questa guida 1
Finalità e destinatari 1
Come usare questo manuale 1
Convenzioni usate in questo manuale 1
Convenzioni tipografiche 1
Avvertenze 2
Richiesta di commenti 2
1. Che cos'è Bitdefender Mobile Security for iOS 4
2. Iniziare 5
2.1. Requisiti dispositivo 5
2.2. Installare Bitdefender Mobile Security for iOS 5
2.3. Accedi al tuo account Bitdefender 6
2.4. Dashboard 7
3. Caratteristiche e funzionalità 9
3.1. Esamina 9
3.2. Protezione web 9
3.2.1. Avvisi di Bitdefender 10
3.3. VPN 11
3.3.1. Abbonamenti 13
3.4. Privacy dell'account 14
4. Informazioni su Bitdefender Central 16
4.1. Accedere a Bitdefender Central 16
4.2. Autenticazione a due fattori 17
4.2.1. Attivare l'autenticazione a due fattori 17
4.3. Aggiungere dispositivi affidabili 18
4.4. I miei dispositivi 19
4.4.1. Aggiungere un nuovo dispositivo 19
4.4.2. Personalizza il tuo dispositivo 20
4.4.3. Azioni in remoto 21
4.5. Attività 22
4.6. I miei abbonamenti 23
4.6.1. Controllare gli abbonamenti disponibili 23
4.6.2. Attiva abbonamento 23
4.6.3. Rinnova abbonamento 24
4.7. Notifiche 25
5. Domande frequenti 26
6. Ottenere aiuto 27
6.1. Richiesta d'aiuto 27
6.2. Risorse online 27

6.2.1. Centro di supporto di Bitdefender 27
6.2.2. La community di esperti di Bitdefender 28
6.2.3. Bitdefender Cyberpedia 28
6.3. Informazioni di contatto 29
6.3.1. Distributori locali 29
Glossario 30

INFORMAZIONI SU QUESTA GUIDA

Finalità e destinatari

Il presente manuale è rivolto a tutti gli utenti iOS che hanno scelto Bitdefender Mobile Security for iOS come soluzione di sicurezza per i propri dispositivi mobili. Le informazioni presentate in questo manuale sono adatte non solo a chi ha un background tecnico, ma a chiunque sia in grado di utilizzare i dispositivi mobili Apple.

Scoprirai come configurare e utilizzare Bitdefender Mobile Security for iOS per proteggerti dalle minacce e dalle altre applicazioni dannose. Inoltre, apprenderai come sfruttare al meglio Bitdefender.

Buona lettura e speriamo che lo troverai utile.

Come usare questo manuale

Questo manuale presenta alcuni argomenti principali:

Iniziare (pagina 5)

Inizia a usare Bitdefender Mobile Security for iOS e la sua interfaccia utente.

Caratteristiche e funzionalità (pagina 9)

Scopri come utilizzare Bitdefender Mobile Security for iOS per proteggerti dalle minacce e dalle applicazioni dannose, apprendendone le funzionalità e caratteristiche.

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. CHE COS'È BITDEFENDER MOBILE SECURITY FOR IOS

Attività online come pagare le bollette, prenotare le vacanze o acquistare beni o servizi, sono molto comode e pratiche. Ma come molte attività che si sono sviluppate su Internet, possono comportare dei rischi, se si ignorano alcune norme di sicurezza, che potrebbero condurre alla compromissione dei propri dati personali. E cosa c'è di più importante del proteggere i dati memorizzati negli account online e nel proprio smartphone?

Bitdefender Mobile Security for iOS ti consente di:

- Offre la più potente protezione dalle minacce con il minimo impatto sulla batteria
- Proteggi i tuoi dati personali: password, indirizzo, informazioni finanziari e dei social
- Controlla facilmente la sicurezza del tuo telefono per rilevare e risolvere eventuali configurazioni errate che potrebbero esporlo
- Evita l'esposizione accidentale dei dati e l'uso improprio per tutte le app installate
- Esamina il tuo dispositivo per ottenere le impostazioni di privacy e sicurezza ottimali
- Ottieni informazioni dettagliate sull'utilizzo delle tue attività online e la cronologia degli incidenti impediti
- Verifica se i tuoi account online sono stati coinvolti in fughe o violazioni dei dati
- Cifra il traffico Internet con la VPN inclusa

Bitdefender Mobile Security for iOS è disponibile gratuitamente e richiede l'attivazione con un account Bitdefender. Tuttavia, l'accesso e l'utilizzo di alcune funzionalità importanti di Bitdefender, come il modulo "Protezione web", richiedono un abbonamento a pagamento.

2. INIZIARE

2.1. Requisiti dispositivo

Bitdefender Mobile Security for iOS funziona su qualsiasi dispositivo con il sistema operativo iOS 11.2 o successivo e richiede una connessione attiva a Internet per essere attivato e rilevare se si è verificata una perdita di dati nei tuoi account online.

2.2. Installare Bitdefender Mobile Security for iOS

- **Da Bitdefender Central**
  - Su iOS
    1. Accedi a **Bitdefender Central**.
    2. Seleziona la scheda **I miei dispositivi**.
    3. Tocca **INSTALLA PROTEZIONE** e poi tocca **Proteggi questo dispositivo**.
    4. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, tocca il pulsante corrispondente.
    5. Sei stato reindirizzato alla app di **App Store**. Nella schermata di App Store, tocca l'opzione di installazione.
  - Su Windows, macOS, Android
    1. Accesso Bitdefender centrale.
    2. Seleziona il **I miei dispositivi** pannello.
    3. Premi **INSTALLA LA PROTEZIONE** e poi premi **Proteggi altri dispositivi**.
    4. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, premi il pulsante corrispondente.
    5. Premi **INVIA LINK DI DOWNLOAD**.
    6. Inserisci l'indirizzo email nel campo corrispondente e premi **INVIA EMAIL**. Nota che il link del download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.

7. Sul dispositivo su cui vuoi installare Bitdefender, controlla l'account email che hai digitato e poi premi il pulsante di download corrispondente.

- **Da App Store**
  Cerca Bitdefender Mobile Security for iOS per localizzare e installare la app.

La prima volta che apri la app, viene visualizzata una finestra di introduzione contenente maggiori dettagli sulle funzionalità del prodotto. Tocca Iniziare per passare alla finestra successiva.

Prima di passare alle diverse fasi per la convalida, devi accettare l'Accordo di abbonamento. Prenditi qualche istante per leggere l'Accordo di abbonamento in quanto contiene i termini e le condizioni con cui è possibile utilizzare Bitdefender Mobile Security for iOS.

Tocca **Continua** per passare alla finestra successiva.

2.3. Accedi al tuo account Bitdefender

Per usare Bitdefender Mobile Security for iOS, devi collegare il tuo dispositivo a un account di Bitdefender, Facebook, Google, Apple o Microsoft, accedendo all'account direttamente dalla app. La prima volta che apri l'applicazione, ti sarà chiesto di accedere a un account.

Per collegare il tuo dispositivo a un account di Bitdefender:

1. Inserisci l'indirizzo e-mail del tuo account Bitdefender nel campo corrispondente e tocca **AVANTI**. Se non hai un account Bitdefender e vuoi crearne uno, seleziona il link corrispondente e segui le istruzioni sullo schermo fino all'attivazione dell'account.
   Per accedere utilizzando un account Facebook, Google, Apple, o Microsoft, tocca il servizio che vuoi utilizzare dall'area **O accedi con**. Sarai reindirizzato alla pagina di accesso del servizio selezionato. Segui le istruzioni per collegare il tuo account a Bitdefender Mobile Security for iOS.

> **Nota**
> Bitdefender non accede ad alcuna informazione confidenziale, come la password dell'account con cui accedi o le informazioni personali dei tuoi amici e contatti.

2. Inserisci la tua password e tocca **ACCEDI**.

Da qui puoi anche accedere all'Informativa sulla privacy di Bitdefender.

2.4. Dashboard

Tocca l'icona di Bitdefender Mobile Security for iOS nell'app drawer del dispositivo per aprire l'interfaccia dell'applicazione.

La prima volta che accedi alla app, ti sarà chiesto di consentire a Bitdefender di inviarti delle notifiche. Tocca **Consenti** per restare informato ogni volta che Bitdefender ha qualcosa da comunicarti di importante sulla app. Per gestire le notifiche Bitdefender, vai in Impostazioni > Notifiche > Mobile Security.

Per accedere alla sezione che ti serve, tocca l'icona corrispondente nella parte inferiore dello schermo.

Protezione web

Resta al sicuro mentre navighi sul web e ogni volta che app meno sicure cercheranno di accedere a domini non affidabili. Per maggiori informazioni, fai riferimento a Protezione web (pagina 9).

VPN

Ottieni sempre la massima privacy indipendentemente dalla rete a cui ti connetti, mantenendo la tua comunicazione Internet cifrata. Per maggiori informazioni, fai riferimento a VPN (pagina 11).

Privacy dell'account

Scopri se i tuoi account e-mail sono stati violati oppure no. Per maggiori informazioni, fai riferimento a Privacy dell'account (pagina 14).

Per vedere opzioni aggiuntive, tocca l'icona ••• sul tuo dispositivo nella schermata principale dell'applicazione. Compariranno le seguenti opzioni:

- **Ripristina acquisti** - Qui puoi ripristinare gli abbonamenti precedenti che hai acquistato tramite il tuo account di iTunes.
- **Impostazioni** - Qui puoi accedere a:
  - **Impostazioni VPN**
    - **Accordo** - è possibile consultare i termini in base ai quali utilizzi il servizio Bitdefender VPN. Toccando l'opzione **Non sono più**

d'accordo, non potrai utilizzare Bitdefender VPN almeno finché non toccherai **Accetto**.

- **Avviso Wi-Fi pubblico** - Puoi attivare o disattivare la notifica del prodotto che compare ogni volta che ti connetti a una rete Wi-Fi non sicura.
  Lo scopo di questa notifica è aiutarti a mantenere i tuoi dati sempre privati e protetti usando Bitdefender VPN.

- **Impostazioni Protezione web**
  - **Accordo** - è possibile consultare i termini in base ai quali utilizzi il servizio Protezione web di Bitdefender. Toccando **Non sono più d'accordo**, non potrai utilizzare Bitdefender VPN almeno finché non toccherai **Accetto**.
  - **Attiva notifica di Protezione web** - Ti avvisa che Protezione web può essere attivata dopo aver completato una sessione di VPN.
- **Rapporti sul prodotto**

- **Feedback** - Da qui puoi lanciare il client email predefinito per inviarci un tuo feedback sulla app.
- **Info app** - Da qui, puoi accedere a varie informazioni sulla versione installata e l'Accordo di abbonamento, l'Informativa sulla privacy e gli accordi per le licenze open-source.

3. CARATTERISTICHE E FUNZIONALITÀ

3.1. Esamina

Bitdefender Mobile Security for iOS ti consente di esaminare il tuo dispositivo per rilevare eventuali vulnerabilità di sicurezza e potenziali minacce. Eseguendo la scansione controllerai:

- **Versione del SO:** controllo della versione di iOS per gli aggiornamenti più recenti.
- **Codice di sblocco/Biometrica:** controllo del livello di sicurezza per l'accesso al dispositivo.
- **Protezione web:** controllo dello stato del modulo Protezione web
- **Privacy dell'account:** controllo della presenza di account monitorati elencati nel modulo Privacy dell'account.
- **Scansione Wi-Fi:** controllo dello stato di sicurezza della rete a cui si è attualmente connessi.

Lo stato di protezione viene determinato dopo che esegui una scansione manuale.

Dopo aver eseguito la prima scansione, visualizzerai i suggerimenti di Autopilot di Bitdefender. Si tratta del tuo consulente di sicurezza personale, che ti fornisce suggerimenti contestuali e basati sull'uso e sulle esigenze del tuo dispositivo. In questo modo, potrai beneficiare di tutto ciò che la tua app ha da offrirti.

> **Nota**
> Quando accedi per la prima volta alla app, ti sarà chiesto di eseguire una scansione.

3.2. Protezione web

Protezione web di Bitdefender garantisce un'esperienza di navigazione sicura avvisandoti di pagine web potenzialmente dannose e quando app installate meno sicure cercheranno di accedere a domini non affidabili.

Quando un URL porta a un sito web noto per essere fraudolento o phishing, o a contenuti dannosi come spyware o virus, la pagina web

viene bloccata, mostrando un avviso. La stessa cosa accade quando le app installate cercano di accedere a domini dannosi.

> **Importante**
> Se ti trovi in un'area in cui l'uso di un servizio VPN è vietato per legge, la funzionalità Protezione web non sarà disponibile.

Per attivare Protezione web:

1. Tocca l'icona nella parte inferiore dello schermo.
2. Tocca **Accetto**.
3. Attiva l'interruttore della Protezione web.

> **Nota**
> La prima volta che attivi Protezione web, ti viene chiesto di consentire a Bitdefender di impostare le configurazioni VPN che monitoreranno il traffico di rete. Tocca **Consenti** per continuare. Se per proteggere il tuo smartphone è stato impostato un metodo di autenticazione (come impronta digitale o codice PIN), dovrai utilizzarlo. Per rilevare l'accesso a domini non affidabili, Protezione web collabora con i servizi VPN.

> **Importante**
> Protezione web e VPN non possono funzionare contemporaneamente. Ogni volta che una delle due viene attivata, l'altra (se in quel momento è attiva) sarà disattivata.

3.2.1. Avvisi di Bitdefender

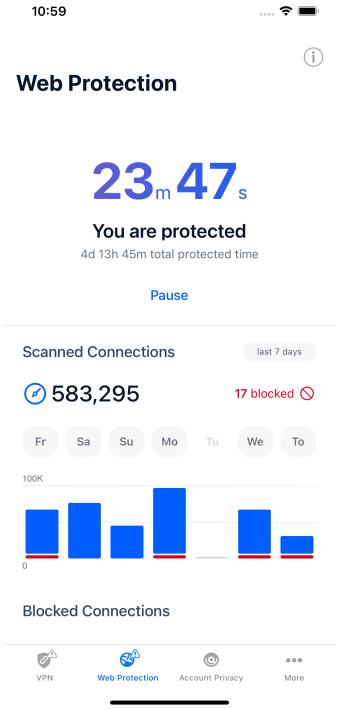
Ogni volta che visiti un sito web classificato come non sicuro, questo viene bloccato. Per informarti dell'evento, vieni avvisato da Bitdefender nel Centro notifiche e nel tuo browser. La pagina di avviso contiene informazioni come l'URL del sito web e la minaccia rilevata. Dunque, dovrai decidere cosa fare.

Inoltre, nel Centro notifiche sarai avvisato ogni volta che una app meno sicura prova ad accedere a domini non affidabili. Tocca la notifica mostrata per essere reindirizzato alla finestra dove potrai decidere cosa fare.

Le seguenti opzioni sono disponibili per entrambi i casi:

- Allontanati dal sito web toccando **RIPORTAMI ALLA PROTEZIONE**.
- Procedi al sito web, malgrado l'avviso, toccando la notifica mostrata e poi su **Voglio accedere alla pagina**.

Conferma la tua scelta.



3.3. VPN

Con Bitdefender VPN puoi mantenere privati i tuoi dati ogni volta che ti connetti a reti wireless non protette mentre sei in aeroporti, centri commerciali, bar o alberghi. In questo modo, è possibile evitare situazioni spiacevoli, come furti di dati personali o tentativi di rendere accessibile il tuo indirizzo IP a pirati informatici.

Il VPN opera come una sorta di tunnel tra il tuo dispositivo e la rete a cui ti connetti, proteggendo la tua connessione, cifrando i dati usando una cifratura di livello militare e nascondendo il tuo indirizzo IP, ovunque ti trovi. Il tuo traffico viene reindirizzato a un server indipendente, rendendo

quindi il tuo dispositivo impossibile da identificare dal tuo provider di servizi Internet tra la miriade di altri dispositivi che stanno usando i nostri servizi. Inoltre, mentre ti connetti a Internet tramite Bitdefender VPN, puoi accedere a contenuti che normalmente sono limitati ad alcuni paesi.

> **Nota**
> Alcuni paesi applicano una censura di Internet e quindi l'utilizzo delle VPN sul loro territorio è proibito per legge. Per evitare conseguenze legali, potrebbe comparire un messaggio di avviso quando cerchi di usare la app Bitdefender VPN per la prima volta. Continuando a utilizzare la app, confermi di essere consapevole dei regolamenti applicabili del paese in cui ti trovi e dei rischi a cui potresti andare incontro.

Per attivare Bitdefender VPN:

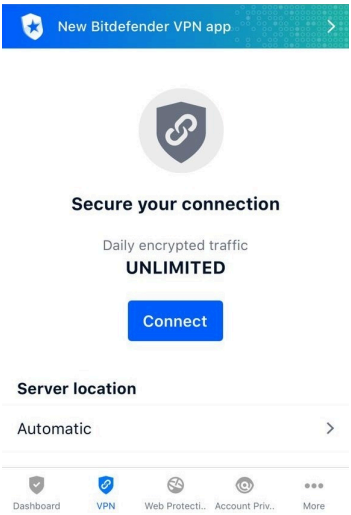
1. Clicca il icona dalla parte inferiore dello schermo.
2. Tocca **Connetti** ogni volta che vuoi restare protetto mentre usi una connessione a reti wireless non affidabili.
   Tocca **Disconnetti** ogni volta che vuoi disattivare la connessione.

> **Nota**
> La prima volta che attivi VPN, ti viene chiesto di consentire a Bitdefender di impostare le configurazioni VPN che monitoreranno il traffico di rete. Tocca **Consenti** per continuare. Se per proteggere il tuo smartphone è stato impostato un metodo di autenticazione (come impronta digitale o codice PIN), dovrai utilizzarlo.

Quando la VPN è attiva, nella barra di stato compare l'icona VPN.

Per risparmiare la batteria, ti consigliamo di disattivare VPN quando non ti serve.

Se hai un abbonamento premium e ti piacerebbe connetterti a un server a tuo piacimento, tocca Automatico nell'interfaccia VPN e poi seleziona l'ubicazione desiderata. Per maggiori dettagli sugli abbonamenti a VPN, fai riferimento a Abbonamenti (pagina 13).



3.3.1. Abbonamenti

Bitdefender VPN offre gratuitamente una quota di traffico giornaliera di 200 MB per proteggere la tua connessione ogni volta che ti serve, connettendoti automaticamente all'ubicazione del server ottimale.

Per ottenere traffico illimitato e accesso senza restrizioni a contenuti in tutto il mondo scegliendo l'ubicazione del server che preferisci, fai l'upgrade alla versione premium.

Puoi fare l'upgrade alla versione Bitdefender Premium VPN in qualunque momento toccando il pulsante **Attiva Premium VPN** disponibile nella finestra di VPN. Puoi scegliere fra due tipi di abbonamento: annuale e mensile.

L'abbonamento Bitdefender Premium a VPN è indipendente dall'abbonamento gratuito a Bitdefender Mobile Security for iOS, il che significa che potrai usarlo per la sua intera disponibilità. Se l'abbonamento Bitdefender Premium a VPN scadesse, sarai riportato automaticamente al piano gratuito.

Bitdefender VPN è un prodotto multipiattaforma, disponibile nei prodotti Bitdefender compatibili con Windows, macOS, Android e iOS. Una volta effettuato l'upgrade al piano premium, potrai usare il tuo abbonamento su tutti i prodotti, a condizione che tu acceda con lo stesso account Bitdefender.

> **Nota**
> Bitdefender VPN funziona anche come applicazione indipendente su tutti i sistemi operativi supportati, ovvero Windows, macOS, Android e iOS.

3.4. Privacy dell'account

Privacy dell'account di Bitdefender rileva se si sono verificate perdite di dati negli account che utilizzi per fare pagamenti e acquisti online, o per accedere a diversi siti web e app online. I dati che potrebbero essere stati memorizzati in un account possono essere password, dati della carta di credito o informazioni bancarie, e, se non protetti correttamente, potrebbero verificarsi furti d'identità o invasioni alla privacy.

Lo stato della privacy di un account viene mostrato subito dopo la conferma.

Per verificare se un account è stato violato, tocca **Scansione per violazioni**.

Per iniziare a proteggere le informazioni personali:

1. Clicca il icona dalla parte inferiore dello schermo.
2. Tocca **Aggiungi account**.
3. Inserisci il tuo indirizzo e-mail nel campo corrispondente e tocca **Avanti**.
   Bitdefender deve confermare questo account prima di mostrare informazioni private. Inoltre, viene inviata un'e-mail con un codice di conferma all'indirizzo fornito.
4. Controlla la tua casella di posta e inserisci il codice che hai ricevuto nella sezione **Privacy dell'account** della tua app. Se non riesci a trovare l'e-mail di conferma nei tuoi messaggi in arrivo, controlla anche la cartella dello Spam.
   Viene mostrato lo stato della privacy dell'account confermato.

Se in uno degli account viene rilevata una violazione, ti consigliamo di modificarne la password il prima possibile. Per creare una password sicura, segui questi suggerimenti:

- Deve contenere almeno otto caratteri.
- Includi sia caratteri minuscoli che maiuscoli.

- Aggiungi almeno un numero o simbolo, come #, @, % or !.

Una volta protetto un account coinvolto in una violazione della privacy, puoi confermare le modifiche spuntando le fughe rilevate come **Risolto**. Per farlo:

1. Tocca ··· accanto alla violazione che hai risolto.
2. Tocca **Segna come risolto**.

Quando tutte le violazioni rilevate sono state segnate come Risolte, l'account non apparirà più come violato, almeno fino al rilevamento di una nuova violazione.

4. INFORMAZIONI SU BITDEFENDER CENTRAL

Bitdefender Central è la piattaforma che consente di accedere alle funzioni e ai servizi online del prodotto, oltre a eseguire in remoto alcune importanti funzioni sui dispositivi in cui è stato installato Bitdefender. Puoi accedere al tuo account Bitdefender da qualsiasi computer o dispositivo mobile connesso a Internet, andando su https://central.bitdefender.com o direttamente dalla app Bitdefender Central sui dispositivi Android e iOS.

Per installare la app Bitdefender Central sui tuoi dispositivi:

- **Su Android** - Cerca Bitdefender Central su Google Play e poi scarica e installa la app. Segui i passaggi richiesti per completare l'installazione.
- **Su iOS** - Cerca Bitdefender Central su App Store, e poi scarica e installa la app. Segui i passaggi richiesti per completare l'installazione.

Una volta eseguito l'accesso, puoi utilizzare le seguenti attività:

- Scarica e installa Bitdefender su sistemi operativi Windows, macOS, iOS e Android. I prodotti che è possibile scaricare sono:
  - Bitdefender Mobile Security per iOS
  - Bitdefender Mobile Security for Android
  - Bitdefender Antivirus for Mac
  - La linea di prodotti Windows di Bitdefender
- Gestire e rinnovare i tuoi abbonamenti Bitdefender.
- Aggiungi nuovi dispositivi alla tua rete e gestiscili ovunque ti trovi.

4.1. Accedere a Bitdefender Central

Ci sono due modi per accedere a Bitdefender Central

- Dal tuo browser web:
  1. Apri un browser web su un dispositivo con accesso a internet.
  2. Vai in: https://central.bitdefender.com.
  3. Accedi al tuo account usando il tuo indirizzo e-mail e la tua password.

- Dal tuo dispositivo Android o iOS:
  Apri la app Bitdefender Central che hai installato.

  > **Nota**
  > In questo materiale abbiamo incluso le opzioni che puoi trovare nell'interfaccia web.

4.2. Autenticazione a due fattori

Il metodo dell'autenticazione a due fattori aggiunge un ulteriore livello di sicurezza al tuo account di Bitdefender, richiedendo un codice di autenticazione oltre alle tue credenziali di accesso. In questo modo, potrai impedire il furto del tuo account e proteggerlo da altri tipi di attacchi informatici, come keylogger, forza bruta o attacchi a dizionario.

4.2.1. Attivare l'autenticazione a due fattori

Attivando l'autenticazione a due fattori, renderai il tuo account di Bitdefender molto più sicuro. La tua identità sarà verificata ogni volta che accederai a dispositivi diversi per installare uno dei prodotti Bitdefender, verificare lo stato del tuo abbonamento o eseguire attività in remoto sui tuoi dispositivi.

Per attivare l'autenticazione a due fattori:

1. Accesso Bitdefender centrale.
2. Tocca l'icona in alto a destra dello schermo.
3. Tocca **account Bitdefender** nel menu scorrevole.
4. Seleziona la scheda **Password e sicurezza**.
5. Tocca **COME INIZIARE**.
   Scegli uno dei seguenti metodi:

   - **App Autenticatore** - Usa una app Autenticatore per generare un codice ogni volta che accedi al tuo account di Bitdefender.
     Se vuoi usare una app Autenticatore, ma non sai quale scegliere, è disponibile un elenco con le app di autenticazione consigliate.

     a. Tocca **USA APP AUTENTICATORE** per iniziare.

     b. Per accedere a un dispositivo Android o iOS, usa il tuo dispositivo per esaminare il codice QR.

Per accedere su un portatile o computer, puoi aggiungere manualmente il codice mostrato.
Tocca **CONTINUA**.

c. Inserisci il codice fornito dalla app o quello mostrato nel passaggio precedente e poi tocca **ATTIVA**.

- **E-mail** - ogni volta che accedi al tuo account di Bitdefender, un codice di verifica sarà inviato alla tua casella di posta. Controlla il tuo account e-mail e poi inserisci il codice che hai ricevuto.

  a. Tocca **USA E-MAIL** per iniziare.

  b. Controlla il tuo account e-mail e inserisci il codice fornito.
  Ricordati che hai cinque minuti per controllare il tuo account di posta e inserire il codice generato. Se il tempo dovesse scadere, dovrai generare un nuovo codice seguendo gli stessi passaggi.

  c. Tocca **ATTIVA**.

  d. Ti vengono forniti dieci codici di attivazione. Puoi copiare, scaricare o stampare l'elenco e usarlo se dovessi perdere il tuo indirizzo e-mail o non potrai accedere. Ogni codice può essere usato una sola volta.

  e. Tocca **FATTO**.

Nel caso non volessi più usare l'autenticazione a due fattori:

1. Tocca **DISATTIVA L'AUTENTICAZIONE A DUE FATTORI**.
2. Controlla la tua app o il tuo account e-mail e inserisci il codice che hai ricevuto.
   Se hai scelto di ricevere il codice di autenticazione via e-mail, hai cinque minuti per controllare il tuo account e-mail e inserire il codice generato. Se il tempo dovesse scadere, dovrai generare un nuovo codice seguendo gli stessi passaggi.
3. Conferma la tua scelta.

4.3. Aggiungere dispositivi affidabili

Per assicurarti che solo tu possa accedere al tuo account di Bitdefender, potrebbe servirti un codice. Se vuoi saltare questo passaggio ogni volta

che ti connetti allo stesso dispositivo, ti consigliamo di inserirlo tra i dispositivi affidabili.

Per aggiungere dispositivi ai dispositivi affidabili:

1. Accesso Bitdefender centrale.
2. Clicca il icona nella parte in alto a destra dello schermo.
3. Rubinetto **Account di Bitdefender** nel menu della diapositiva.
4. Seleziona il **Password e sicurezza** scheda.
5. Tocca **dispositivi affidabili**.
6. Viene mostrato l'elenco con i dispositivi su cui è stato installato Bitdefender. Tocca il dispositivo desiderato.

Puoi aggiungere quanti dispositivi desideri, a patto che abbiano installato Bitdefender e che il tuo abbonamento sia valido.

4.4. I miei dispositivi

L'area **I miei dispositivi** nel tuo account Bitdefender ti consente d'installare, gestire e utilizzare in remoto il tuo prodotto Bitdefender su qualsiasi dispositivo, a condizione che sia acceso e connesso a Internet. Le schede del dispositivo mostrano il nome del dispositivo, lo stato di protezione e l'eventuale presenza di rischi che influenzano i dispositivi.

4.4.1. Aggiungere un nuovo dispositivo

Se l'abbonamento copre più di un dispositivo, è possibile aggiungerne un altro e installare Bitdefender Mobile Security for iOS su di esso, come segue:

1. Accesso Bitdefender centrale.
2. Seleziona il **I miei dispositivi** pannello, quindi toccare **INSTALLA LA PROTEZIONE**.
3. Scegli una delle due opzioni disponibili:
   - **Proteggi questo dispositivo**
     Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, tocca il pulsante corrispondente.
   - **Proteggi altri dispositivi**

Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, tocca il pulsante corrispondente.

Clicca su **INVIA LINK DI DOWNLOAD**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA E-MAIL**. Nota che il link di download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.

Sul dispositivo su cui desideri installare il tuo prodotto Bitdefender, controlla l'account e-mail che hai digitato, quindi tocca il pulsante di download corrispondente.

4. Attendi il completamento del download e poi esegui il programma d'installazione.

4.4.2. Personalizza il tuo dispositivo

Per identificare facilmente i tuoi dispositivi, puoi personalizzarne il nome:

1. Accesso Bitdefender centrale.
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca sulla scheda del dispositivo desiderato e poi sull'icona ⋮ nell'angolo in alto a destra dello schermo.
4. Seleziona **Impostazioni**.
5. Inserisci un nuovo nome nel campo **Nome dispositivo** e clicca su **SALVA**.

Puoi creare e assegnare un proprietario a ogni dispositivo per una gestione migliore:

1. Accesso Bitdefender centrale.
2. Seleziona il **I miei dispositivi** pannello.
3. Toccare la scheda del dispositivo desiderato, quindi il ⋮ icona nell'angolo in alto a destra dello schermo.
4. Seleziona **Profilo**.
5. Clicca su **Aggiungi proprietario** e compila i campi corrispondenti. Personalizza il profilo aggiungendo una foto, selezionando una data di nascita e inserendo un indirizzo e-mail e un numero di telefono.

6. Clicca su **AGGIUNGI** per salvare il profilo.
7. Seleziona il proprietario desiderato dall'elenco **Proprietario dispositivo** e clicca su **ASSEGNA**.

4.4.3. Azioni in remoto

Per aggiornare Bitdefender in remoto su un dispositivo:

1. Accesso Bitdefender centrale.
2. Seleziona il **I miei dispositivi** pannello.
3. Toccare la scheda del dispositivo desiderato, quindi il ⋮ icona nell'angolo in alto a destra dello schermo.
4. Seleziona **Aggiorna**.

Per maggiori informazioni e altre azioni in remoto riguardo il tuo prodotto Bitdefender su un determinato dispositivo, clicca sulla scheda del dispositivo desiderato.

Una volta cliccato su una scheda di un dispositivo, saranno disponibili le seguenti schede:

- **Dashboard.** In questa finestra, puoi visualizzare maggiori dettagli sul dispositivo selezionato, controllare il suo stato di protezione, lo stato di Bitdefender VPN e quante minacce sono state bloccate negli ultimi sette giorni. Lo stato di protezione può essere verde, quando nessun problema influenza il dispositivo, giallo, quando il dispositivo richiede le tue attenzioni, e rosso, quando il dispositivo è a rischio. In caso di problemi sul dispositivo, clicca sulla freccia a tendina nella parte superiore dell'area dello stato per scoprire maggiori dettagli. Qui
- **Protezione.** Da questa finestra puoi eseguire una scansione veloce o di sistema sui tuoi dispositivi in modalità remota. Clicca sul pulsante **ESAMINA** per avviare il processo. Puoi anche verificare quando è stata eseguita l'ultima scansione sul dispositivo oltre a un rapporto sulla stessa, con tutte le informazioni più importanti.
- **Ottimizzatore.** Qui puoi migliorare in remoto le prestazioni di un dispositivo esaminando, rilevando e rimuovendo rapidamente i file inutili. Clicca sul pulsante **INIZIA** e seleziona le aree che vuoi ottimizzare. Clicca di nuovo sul pulsante **INIZIA** per avviare il processo di ottimizzazione. Clicca su **Altri dettagli** per accedere a un rapporto dettagliato sui problemi risolti.

- **Anti-Theft.** In caso di smarrimento, perdita o furto, con la funzionalità Anti-Theft puoi localizzare il tuo dispositivo e intraprendere alcune azioni in remoto. Clicca su **LOCALIZZA** per scoprire la sua posizione. Sarà mostrata l'ultima posizione nota, insieme all'ora e alla data.
- **Vulnerabilità.** Per controllare un dispositivo alla ricerca di vulnerabilità, come aggiornamenti di Windows non installati, app datate o password deboli, clicca sul pulsante **ESAMINA** nella scheda Vulnerabilità. Le vulnerabilità non possono essere risolte in remoto. Nel caso fosse rilevata una qualche vulnerabilità, devi eseguire una nuova scansione sul dispositivo e intraprendere tutte le azioni necessarie. Clicca su **Altri dettagli** per accedere a un rapporto dettagliato sui problemi trovati.

4.5. Attività

Nella sezione Attività hai accesso a informazioni sui dispositivi con Bitdefender installato.

Una volta eseguito l'accesso alla finestra **Attività**, saranno disponibili le seguenti schede:

- **I miei dispositivi.** Qui puoi visualizzare il numero di dispositivi connessi accanto al proprio stato di protezione. Per risolvere i problemi in remoto sui dispositivi rilevati, clicca su **Risolvi problemi** e poi su **ESAMINA E RISOLVI I PROBLEMI**.

  Per vedere altri dettagli sui problemi rilevati, clicca su **Vedi problemi**.

  Le informazioni sulle minacce rilevate non possono essere recuperate da dispositivi iOS.
- **Minacce bloccate.** Qui puoi visualizzare un grafico che mostra alcune statistiche generali tra cui informazioni sulle minacce bloccate nelle ultime 24 ore e sette giorni. Le informazioni mostrate vengono recuperate in base al comportamento dannoso rilevato su file, app e URL a cui si accede.
- **Principali utenti con minacce bloccate**. Qui puoi visualizzare un elenco con gli utenti a cui sono state trovate la maggior parte delle minacce.
- **Principali dispositivi con minacce bloccate**. Qui puoi visualizzare un elenco con i dispositivi in cui sono state trovate la maggior parte delle minacce.

4.6. I miei abbonamenti

La piattaforma Bitdefender Central ti dà la possibilità di gestire facilmente gli abbonamenti per tutti i tuoi dispositivi.

4.6.1. Controllare gli abbonamenti disponibili

Per controllare gli abbonamenti disponibili:

1. Accesso Bitdefender centrale.
2. Seleziona il pannello **I miei abbonamenti**.

Qui puoi avere maggiori informazioni sulla disponibilità degli abbonamenti che possiedi e il numero di dispositivi che li utilizzano.

Puoi aggiungere un nuovo dispositivo a un abbonamento o rinnovarlo, selezionando una scheda d'abbonamento.

> **Nota**
> Puoi avere uno o più abbonamenti sul tuo account, a condizione che siano per piattaforme differenti (Windows, macOS, iOS o Android).

4.6.2. Attiva abbonamento

Un abbonamento può essere attivato durante la fase di installazione utilizzando il tuo account Bitdefender. Con il processo di attivazione, il periodo di validità dell'abbonamento inizia a scalare.

Se hai acquistato un codice di attivazione da uno dei nostri rivenditori o l'hai ricevuto come omaggio, puoi aggiungere la sua disponibilità al tuo abbonamento a Bitdefender.

Per attivare un abbonamento utilizzando un codice di attivazione, segui questi passaggi:

1. Accesso Bitdefender centrale.
2. Seleziona il **le mie sottoscrizioni** pannello.
3. Clicca sul pulsante **CODICE DI ATTIVAZIONE** e digita il codice nel campo corrispondente.
4. Clicca su **ATTIVA** per continuare.

Ora l'abbonamento è attivato.

4.6.3. Rinnova abbonamento

Se hai disattivato il rinnovo automatico del tuo abbonamento a Bitdefender, puoi rinnovarlo manualmente seguendo questi passaggi:

1. Accesso Bitdefender centrale.
2. Seleziona il **le mie sottoscrizioni** pannello.
3. Seleziona la scheda di abbonamento desiderata.
4. Clicca su **RINNOVA** per continuare.

Si aprirà una pagina web nel tuo browser, da cui potrai rinnovare il tuo abbonamento a Bitdefender.

4.7. Notifiche

Per aiutarti a ricevere tutte le ultime informazioni su ciò che succede sui dispositivi associati al tuo account, l'icona è sempre a portata di mano. Cliccandoci sopra, ottieni un'immagine che riassume maggiori informazioni sulle attività dei prodotti Bitdefender installati sui tuoi dispositivi.

5. DOMANDE FREQUENTI

In che modo Bitdefender Mobile Security for iOS mi protegge da virus e minacce informatiche?

Bitdefender Mobile Security for iOS fornisce una protezione assoluta da tutte le minacce informatiche ed è stato progettato appositamente per mantenere i tuoi dati al sicuro da occhi indiscreti.

Ottieni una vasta gamma di funzioni avanzate di sicurezza e privacy per il tuo iPhone e iPad, oltre a molte funzioni bonus, tra cui VPN e Protezione web.

Bitdefender Mobile Security for iOS reagisce subito ai virus e malware senza compromettere le prestazioni del sistema.

Che tipo di dispositivi e sistemi operativi sono protetti da Bitdefender Mobile Security for iOS?

Bitdefender Mobile Security per iOS proteggerà i tuoi smartphone e tablet con iOS da tutte le minacce informatiche.

Perché mi serve Bitdefender Mobile Security per iOS su Apple OS?

Alcuni dei tuoi dati più personali sono memorizzati sul tuo iPhone o iPad, e devi sempre avere la certezza che siano al sicuro. Bitdefender Mobile Security for iOS fornisce una protezione totale dalle minacce informatiche e si prende cura della tua privacy online e delle tue informazioni private senza interferire nelle tue attività quotidiane.

Ottengo una VPN con il mio abbonamento a Bitdefender Mobile Security per iOS?

Bitdefender Mobile Security for iOS ha una versione base di Bitdefender VPN, che include una generosa quantità di traffico gratuito (200 MB/giorno, per un totale di 6 GB/mese).

6. OTTENERE AIUTO

6.1. 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.

6.2. 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.

6.2.1. 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/.

6.2.2. 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/

6.2.3. 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/.

6.3. 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/

6.3.1. 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.