

MANUALE D'USO

**Bitdefender**® CONSUMER  
SOLUTIONS

# Mobile Security





# Bitdefender Mobile Security

## Guida dell'utente

Data di pubblicazione 02/10/2023

Diritto d'autore © 2023 Bitdefender

## Avviso legale

**Tutti i diritti riservati.** Nessuna parte di questo libro può essere riprodotta o trasmessa in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, incluse fotocopie, registrazioni o qualsiasi sistema di memorizzazione e recupero di informazioni, senza il permesso scritto di un rappresentante autorizzato di Bitdefender. L'inserimento di brevi citazioni nelle recensioni può essere possibile solo con la menzione della fonte citata. Il contenuto non può essere modificato in alcun modo.

**Avviso e dichiarazione di non responsabilità.** Questo prodotto e la relativa documentazione sono protetti da copyright. Le informazioni contenute in questo documento sono fornite "così come sono", senza garanzia. Sebbene ogni precauzione sia stata presa nella preparazione di questo documento, gli autori non avranno alcuna responsabilità nei confronti di alcuna persona o entità rispetto a qualsiasi perdita o danno causato o presumibilmente causato direttamente o indirettamente dalle informazioni contenute in questo lavoro.

Questo libro contiene collegamenti a siti Web di terze parti che non sono sotto il controllo di Bitdefender, pertanto Bitdefender non è responsabile del contenuto di qualsiasi sito collegato. Se accedi a un sito Web di terze parti elencato in questo documento, lo farai a tuo rischio. Bitdefender fornisce questi collegamenti solo per comodità e l'inclusione del collegamento non implica che Bitdefender approvi o accetti alcuna responsabilità per il contenuto del sito di terze parti.

**Marchi.** I nomi dei marchi possono apparire in questo libro. Tutti i marchi registrati e non registrati in questo documento sono di esclusiva proprietà dei rispettivi proprietari e sono rispettosamente riconosciuti.

**Bitdefender**<sup>®</sup>



# Indice

<b>Informazioni su questa guida .....</b>	<b>1</b>
Finalità e destinatari .....	1
Come usare questo manuale .....	1
Convenzioni usate in questo manuale .....	1
Convenzioni tipografiche .....	1
Avvertenze .....	2
Richiesta di commenti .....	2
<b>1. Cos'è Bitdefender Mobile Security .....</b>	<b>4</b>
<b>2. Iniziare .....</b>	<b>5</b>
2.1. Requisiti dispositivo .....	5
2.2. Installare Bitdefender Mobile Security .....	5
2.3. Accedi al tuo account Bitdefender .....	6
2.4. Configurare la protezione .....	7
2.5. Dashboard .....	7
<b>3. Caratteristiche e funzionalità .....</b>	<b>11</b>
3.1. Scansione malware .....	11
3.1.1. Rilevamento anomalie dell'app .....	13
3.2. Protezione web .....	13
3.3. VPN .....	15
3.3.1. Impostazioni VPN .....	16
3.3.2. Abbonamenti .....	17
3.4. Allerta truffe .....	18
3.4.1. Attivare Allerta truffe .....	19
3.4.2. Protezione chat in tempo reale .....	19
3.5. Funzioni Antifurto .....	20
3.5.1. Attivare Anti-Theft .....	21
3.5.2. Utilizzare le funzioni Anti-Theft da Bitdefender Central .....	23
3.5.3. Impostazioni Anti-Theft .....	24
3.6. Privacy dell'account .....	24
3.7. Blocco App .....	25
3.7.1. Attivare Blocco App .....	26
3.7.2. Modalità Blocco .....	27
3.7.3. Impostazioni Blocco App .....	28
3.7.4. Scatta foto .....	28
3.7.5. Sblocco rapido .....	29
3.8. Rapporti .....	30
3.9. WearON .....	31
3.9.1. Attivare WearON .....	31
3.10. Info .....	32



<b>4. Informazioni su Bitdefender Central</b> .....	<b>33</b>
4.1. Accedere a Bitdefender Central .....	33
4.2. Autenticazione a due fattori .....	34
4.2.1. Attivare l'autenticazione a due fattori .....	34
4.3. Aggiungere dispositivi affidabili .....	36
4.4. I miei dispositivi .....	36
4.4.1. Aggiungere un nuovo dispositivo .....	36
4.4.2. Personalizza il tuo dispositivo .....	37
4.4.3. Azioni in remoto .....	38
4.5. Attività .....	39
4.6. I miei abbonamenti .....	40
4.6.1. Controllare gli abbonamenti disponibili .....	40
4.6.2. Attiva abbonamento .....	40
4.6.3. Rinnova abbonamento .....	41
4.7. Notifiche .....	42
<b>5. Domande frequenti</b> .....	<b>43</b>
<b>6. Ottenere aiuto</b> .....	<b>49</b>
6.1. Richiesta d'aiuto .....	49
6.2. Risorse online .....	49
6.2.1. Centro di supporto di Bitdefender .....	49
6.2.2. La community di esperti di Bitdefender .....	50
6.2.3. Bitdefender Cyberpedia .....	50
6.3. Informazioni di contatto .....	51
6.3.1. Distributori locali .....	51
<b>Glossario</b> .....	<b>52</b>



## INFORMAZIONI SU QUESTA GUIDA

### Finalità e destinatari

Il presente manuale è rivolto a tutti gli utenti Android che hanno scelto Bitdefender Mobile Security 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 Android.

Scoprirai come configurare e utilizzare Bitdefender Mobile Security per proteggerti dalle minacce e dalle altre applicazioni dannose. Inoltre, apprendrai 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 e la sua interfaccia utente.

[Caratteristiche e funzionalità \(pagina 11\)](#)

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

[Ottenere aiuto \(pagina 49\)](#)

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.
<a href="https://www.bitdefender.com">https://www.bitdefender.com</a>	I link URL indirizzano a una qualche ubicazione esterna, su server http o ftp.
<a href="mailto:documentation@bitdefender.com">documentation@bitdefender.com</a>	Gli indirizzi e-mail vengono inseriti nel testo come informazioni di contatto.
<a href="#">A proposito di questa guida (pagina 1)</a>	Questo è un link interno, verso una qualche ubicazione nel documento.
filename	File e directory vengono stampati utilizzando monospaced font.
<b>opzione</b>	Tutte le opzioni del prodotto vengono stampate utilizzando <b>grassetto</b> caratteri.
<b>parola chiave</b>	Le parole chiave o le frasi importanti vengono evidenziate utilizzando <b>grassetto</b> 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](mailto: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 MOBILE SECURITY

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** ti consente di:

- Ottenere la migliore protezione per il tuo tablet e smartphone Android con un impatto minimo sulla durata della batteria
- Non cadere vittima delle truffe mobile basate sui link
- Accedere alla tua VPN sicura per un'esperienza di navigazione web sempre veloce, anonima e sicura
- Localizzare, bloccare e azzerare in remoto il tuo dispositivo Android in caso di furto o smarrimento
- Verificare se il tuo account di posta elettronica è stato coinvolto in violazioni o fughe di dati





## 2. INIZIARE

### 2.1. Requisiti dispositivo

Bitdefender Mobile Security funziona su ogni dispositivo con Android 5.0 e una versione successiva. Per la scansione delle minacce nel cloud serve una connessione a Internet attiva.

### 2.2. Installare Bitdefender Mobile Security

#### ○ Da Bitdefender Central

##### ○ Su Android

1. Vai in: <https://central.bitdefender.com>.
2. Accedi al tuo account Bitdefender.
3. Seleziona la scheda **I miei dispositivi**.
4. Tocca **INSTALLA LA PROTEZIONE** e poi tocca **Proteggi questo dispositivo**.
5. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, tocca il pulsante corrispondente.
6. Sarai reindirizzato alla app su **Google Play**. Nella schermata di Google Play, tocca l'opzione di installazione.

##### ○ Su Windows, macOS e iOS

1. Vai a: <https://central.bitdefender.com>.
2. Accedi al tuo account Bitdefender.
3. Seleziona il **I miei dispositivi** pannello.
4. Premi **INSTALLA LA PROTEZIONE** e poi premi **Proteggi altri dispositivi**.
5. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, premi il pulsante corrispondente.
6. Premi **INVIA LINK DI DOWNLOAD**.
7. Inserisci l'indirizzo e-mail nel campo corrispondente e premi **INVIA E-MAIL**. 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.

8. Sul dispositivo su cui vuoi installare Bitdefender, controlla l'account e-mail che hai inserito e premi il pulsante di download corrispondente.

### ○ Da Google Play

Cerca Bitdefender Mobile Security per localizzare e installare la app. In alternativa, inquadra il codice QR:



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.

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

## 2.3. Accedi al tuo account Bitdefender

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

Se hai installato Bitdefender Mobile Security dal tuo account Bitdefender, la app tenterà di accedere automaticamente a tale account.

Per collegare il tuo dispositivo a un account di Bitdefender:

1. Inserisci l'indirizzo e-mail e la password del tuo account di Bitdefender nei campi corrispondenti. Se non hai un account di Bitdefender e vuoi crearne uno, seleziona il link corrispondente.
2. Tocca **ACCEDI**.

Per accedere utilizzando un account Facebook, Google 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.



### 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.

## 2.4. Configurare la protezione

Una volta eseguito l'accesso alla app, comparirà la finestra Configura la protezione. Per proteggere il tuo dispositivo, ti consigliamo di seguire questi passaggi:

- **Stato dell'abbonamento.** Per ottenere la protezione da Bitdefender Mobile Security, devi attivare il prodotto con un abbonamento, che specifica per quanto tempo puoi utilizzarlo. alla scadenza, la app smette di eseguire le proprie funzioni e proteggere il tuo dispositivo. Se hai un codice di attivazione, tocca **HO UN CODICE** e poi tocca **ATTIVA**.  
Se hai eseguito l'accesso con un nuovo account di Bitdefender e non hai un codice di attivazione, puoi usare il prodotto per 14 giorni gratuitamente.
- **Protezione web.** Se il tuo dispositivo richiede l'accessibilità per attivare Protezione web, tocca **ATTIVA**. Si aprirà il menu dell'accessibilità. Tocca Bitdefender Mobile Security e attiva l'interruttore corrispondente.
- **Scansione malware.** Esegui una scansione unica per assicurarti che il tuo dispositivo sia privo di minacce. Per avviare il processo di scansione, tocca **ESAMINA ORA**.  
Non appena il processo di scansione inizierà, comparirà la dashboard. Qui puoi visualizzare lo stato di sicurezza del tuo dispositivo.

## 2.5. Dashboard

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

La dashboard offre informazioni sullo stato di sicurezza del tuo dispositivo e tramite Autopilot ti aiuta a migliorare la sua sicurezza dandoti suggerimenti sulle varie funzionalità.



La scheda stato nella parte superiore della finestra ti informa sullo stato di sicurezza del dispositivo usando messaggi chiari e colori indicativi. Se Bitdefender Mobile Security non ha alcun avviso, la scheda dello stato è verde. Quando viene rilevato un problema di sicurezza, la scheda dello stato diventa rossa.

Per offrirti un funzionamento efficace e una maggiore protezione mentre esegui diverse attività, **Bitdefender Autopilot** agirà come tuo consulente di sicurezza personale. In base alle attività eseguite, sia che tu stia lavorando o effettuando pagamenti online, Bitdefender Autopilot ti fornirà suggerimenti contestuali basati sull'uso e le esigenze del tuo dispositivo. Ciò ti aiuterà a scoprire e usufruire dei vantaggi offerti dalle funzionalità incluse nella app Bitdefender Mobile Security.

Ogni volta che vi è un processo in esecuzione o una funzione richiede un tuo intervento, nell'interfaccia viene mostrata una scheda con maggiori informazioni e le possibili azioni.

Puoi accedere alle funzionalità di Bitdefender Mobile Security e selezionarle facilmente dalla barra di navigazione in basso:

### **Scansione malware**

Ti consente di avviare una scansione a richiesta e attivare la funzione Esamina la memoria. Per maggiori informazioni, fai riferimento a [Scansione malware \(pagina 11\)](#).

### **Protezione web**

Assicura una navigazione sicura, avvisandoti in caso di eventuali pagine web potenzialmente dannose. Per maggiori informazioni, fai riferimento a [Protezione web \(pagina 13\)](#).

### **VPN**

Cifra le comunicazioni via Internet, aiutandoti a mantenere la tua privacy, indipendentemente dalla rete a cui ci si connette. Per maggiori informazioni, fai riferimento a [VPN \(pagina 15\)](#).

### **Allerta truffe**

Ti mantiene al sicuro avvisandoti dell'arrivo di collegamenti dannosi ricevuti tramite SMS, applicazioni di messaggistica e qualsiasi tipo di notifica. Per maggiori informazioni, fai riferimento a [Allerta truffe \(pagina 18\)](#).

### **Anti-Theft**



Ti consente di attivare o disattivare le funzioni antifurto e di configurarne le relative impostazioni. Per maggiori informazioni, fai riferimento a [Funzioni Antifurto \(pagina 20\)](#).

### **Privacy dell'account**

Verifica se nei tuoi account online si è verificata un'eventuale violazione dei dati. Per maggiori informazioni, fai riferimento a [Privacy dell'account \(pagina 24\)](#).

### **Blocco App**

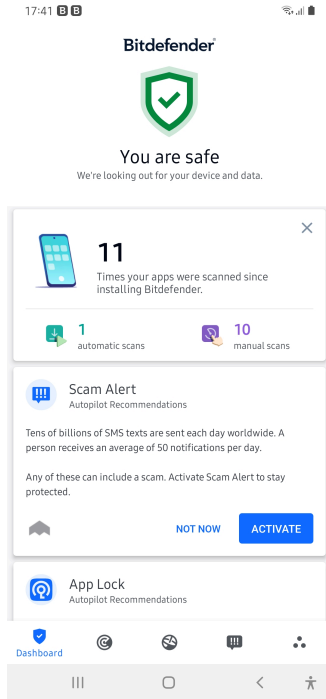
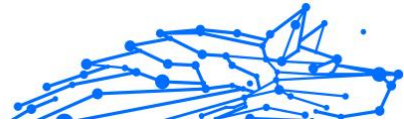
Ti consente di proteggere le applicazioni installate impostando un codice di accesso PIN. Per maggiori informazioni, fai riferimento a [Blocco App \(pagina 25\)](#).

### **Rapporti**

Mantiene un registro di tutte le azioni importanti, i cambiamenti di stato e altri messaggi critici relativi alle attività del tuo dispositivo. Per maggiori informazioni, fai riferimento a [Rapporti \(pagina 30\)](#).

### **WearON**

Comunica con il tuo smartwatch per aiutarti a trovare il telefono nel caso l'avessi smarrito o dimenticato dove l'hai lasciato. Per maggiori informazioni, fai riferimento a [WearON \(pagina 31\)](#).





## 3. CARATTERISTICHE E FUNZIONALITÀ

### 3.1. Scansione malware

Bitdefender protegge il tuo dispositivo e i tuoi dati da applicazioni dannose usando una scansione all'installazione e a richiesta.

L'interfaccia dello scanner per malware fornisce un elenco di tutti i tipi di minacce cercate da Bitdefender, oltre alle loro definizioni. Tocca semplicemente una minaccia per visualizzarne la definizione.



#### Nota

Assicurati che il dispositivo mobile sia connesso a Internet. Se il dispositivo non è connesso a Internet, la scansione non inizierà.

#### ○ Scansione all'installazione


Ogni volta che si installa un'applicazione, Bitdefender Mobile Security esegue automaticamente una scansione utilizzando la tecnologia in-the-cloud. Lo stesso processo di scansione viene avviato ogni volta che le app installate sono aggiornate.

Se l'applicazione viene giudicata pericolosa, un avviso ti segnalerà di disinstallarla. Tocca **Disinstalla** per accedere alla schermata di disinstallazione dell'applicazione.

#### ○ Scansione a richiesta

Ogni volta che vuoi assicurarti che le applicazioni installate sul dispositivo siano sicure, puoi avviare una scansione a richiesta.

Per avviare una scansione a richiesta:

1. Tocca  **Scansione malware** nella barra di navigazione in basso.
2. Tocca **AVVIA SCANSIONE**.



### Nota



In Android 6, per la funzione Scansione malware sono richieste alcune autorizzazioni aggiuntive. Dopo aver toccato il pulsante **AVVIA SCANSIONE**, seleziona **Consenti** per le seguenti opzioni:

- Consenti ad **Antivirus** di effettuare e gestire le chiamate?
- Consenti ad **Antivirus** di accedere a foto, filmati e file sul tuo dispositivo?

Puoi visualizzare l'avanzamento della scansione ed eventualmente fermarla in qualsiasi momento.


Di norma, Bitdefender Mobile Security esaminerà la memoria di archiviazione interna del dispositivo, incluso eventuali schede SD inserite. In questo modo, qualsiasi applicazione pericolosa che potrebbe trovarsi sulla scheda può essere rilevata prima ancora di provocare danni.

Per disattivare la funzione Esamina la memoria:

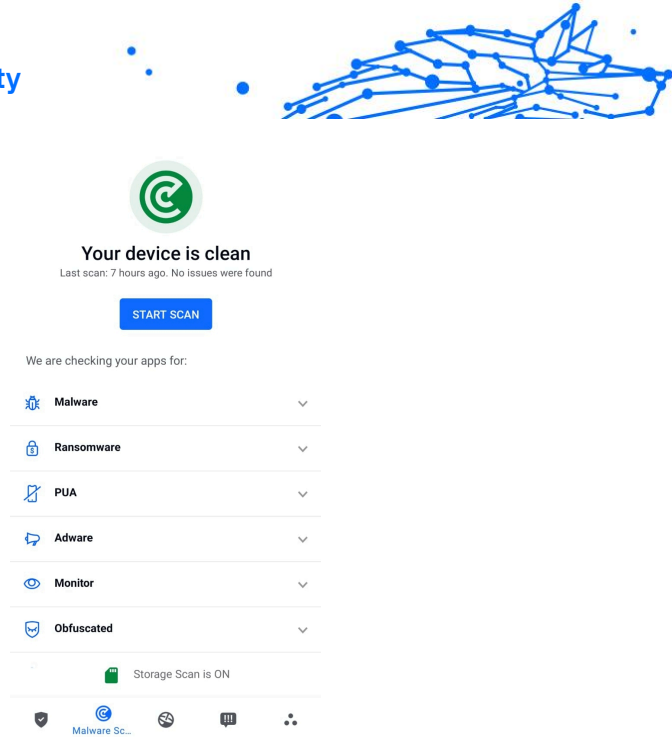
1. Tocca  **Altro** nella barra di navigazione in basso.
2. Tocca  **Impostazioni**.
3. Disattiva l'interruttore **Esamina la memoria** nell'area Scansione malware.

Se viene rilevata un'eventuale applicazione dannosa, saranno mostrate ulteriori informazioni e potrai rimuoverla, toccando il pulsante **DISINSTALLA**.

La scheda Scansione malware mostra lo stato del tuo dispositivo. Quando il dispositivo è protetto, la scheda è verde, mentre diventerà rossa, se il dispositivo richiede una scansione o in caso di eventuali azioni che necessitano di un tuo intervento.

Se la tua versione di Android è 7.1 o superiore, puoi accedere a un collegamento allo Scanner malware così da poter eseguire scansioni più velocemente, senza aprire l'interfaccia di Bitdefender Mobile Security. Per farlo, tieni premuta l'icona di Bitdefender nella schermata Home o nell'app drawer, e seleziona l'icona .





## 3.1.1. Rilevamento anomalie dell'app

Bitdefender App Anomaly Detection è una nuova tecnologia integrata nello scanner malware Bitdefender per fornire un ulteriore livello di protezione monitorando e rilevando continuamente eventuali comportamenti dannosi e avvisando l'utente se vengono identificate attività sospette.

Il rilevamento anomalie dell'app Bitdefender protegge gli utenti anche quando hanno inconsapevolmente installato un'app pericolosa che rimane inattiva per un periodo di tempo o un'app apparentemente affidabile che ne interrompe la funzionalità e diventa canaglia.

## 3.2. Protezione web

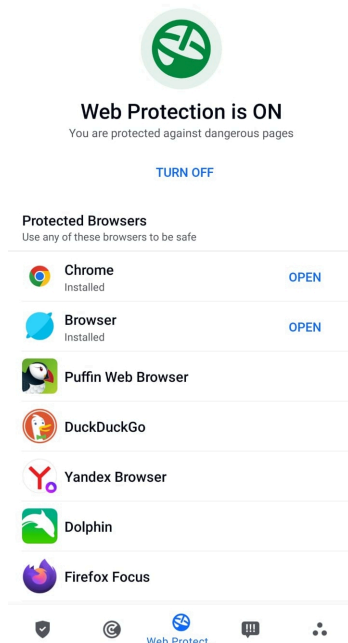
Utilizzando i servizi cloud di Bitdefender, Protezione web esamina le pagine web a cui accedi con il browser predefinito di Android, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser e Dolphin.



## Nota



In Android 6, per la funzione Protezione web sono richieste alcune autorizzazioni aggiuntive.

Consenti di registrare il servizio di accessibilità e tocca **ATTIVA** quando richiesto. Tocca **Antivirus** e attiva l'interruttore, poi conferma di essere d'accordo con l'accesso all'autorizzazione del dispositivo.



Protezione web di Bitdefender è impostata per avisarti di utilizzare Bitdefender VPN ogni volta che accedi a un sito bancario. La notifica compare nella barra di stato. Ti consigliamo di usare Bitdefender VPN mentre usi il tuo account bancario così da proteggere i tuoi dati da potenziali violazioni di sicurezza.

Per disattivare la notifica di Protezione web:

1. Rubinetto  **Di più** nella barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.



3. disattiva il corrispondente interruttore nell'area Protezione web.

### 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 tipo bancario e nascondendo il tuo indirizzo IP, ovunque ti trovi. Il tuo traffico viene reindirizzato a un server indipendente, rendendo quindi il tuo dispositivo quasi impossibile da identificare tra la miriade di altri dispositivi che stanno usando i nostri servizi. Inoltre, mentre ti connetti a Internet tramite 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 nel paese in cui ti trovi e dei rischi a cui potresti andare incontro.

Ci sono due modi per attivare o disattivare Bitdefender VPN:

- Tocca **CONNETTI** nella scheda VPN della Dashboard.  
Viene mostrato lo stato di Bitdefender VPN.
- Tocca  **VPN** nella barra di navigazione in basso e poi tocca **CONNETTI**.  
Tocca **CONNETTI** ogni volta che vuoi restare al sicuro mentre usi la connessione a reti wireless non affidabili.  
Tocca **DISCONNETTI** ogni volta che vuoi disattivare la connessione.




#### Nota

La prima volta che attivi VPN, ti verrà chiesto di consentire a Bitdefender di impostare una connessione VPN, che monitorerà il traffico di rete. Tocca **OK** per continuare.

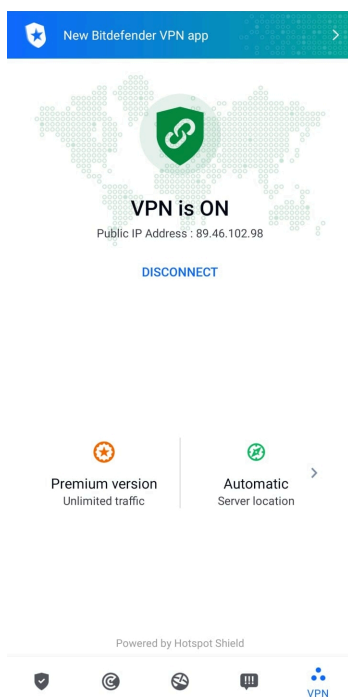


Se la versione del tuo sistema Android è 7.1 o superiore, puoi accedere a una scorciatoia per Bitdefender VPN, senza aprire l'interfaccia di Bitdefender Mobile Security.

Per farlo, tieni premuta l'icona di Bitdefender nella schermata Home o nell'app drawer e seleziona l'icona .

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



Se hai un abbonamento premium e ti piacerebbe connetterti a un server a tuo piacimento, tocca Posizione server nella funzionalità VPN e poi seleziona l'ubicazione desiderata. Per maggiori dettagli sugli abbonamenti a VPN, fai riferimento a



### 3.3.1. Impostazioni VPN

Per una configurazione avanzata della tua VPN:



1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.

Nell'area VPN, puoi configurare le seguenti opzioni:

- Accesso rapido a VPN - Nella barra di stato del tuo dispositivo comparirà una notifica per consentirti di attivare rapidamente VPN.
- Avviso rete Wi-Fi aperta - Ogni volta che ti connetti a una rete Wi-Fi aperta, ti verrà segnalato nella barra di stato del tuo dispositivo di usare VPN.

### 3.3.2. 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 a Bitdefender Premium VPN in qualsiasi momento toccando **Attiva Premium** nella finestra VPN.

L'abbonamento a Bitdefender Premium VPN è indipendente dall'abbonamento a Bitdefender Mobile Security, ciò significa che potrai utilizzarlo per tutta la sua disponibilità, indipendentemente dallo stato del tuo abbonamento di sicurezza. Nel caso l'abbonamento a Bitdefender Premium VPN fosse scaduto, ma quello a Bitdefender Mobile Security fosse ancora attivo, tornerai al piano gratuito.

Bitdefender VPN è un prodotto multiplatforma, 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.

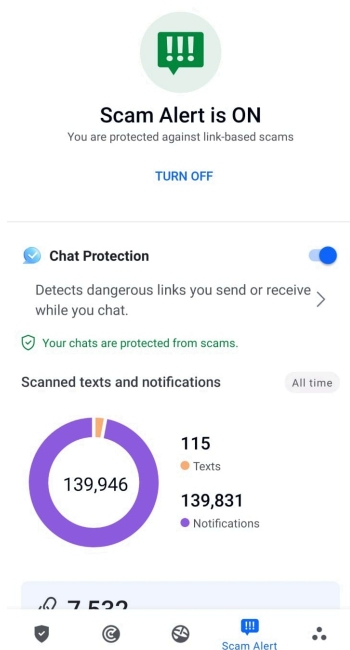


## 3.4. Allerta truffe

La funzionalità Allerta truffe prende misure preventive in prima linea, affrontando situazioni potenzialmente pericolose prima ancora che abbiano la possibilità di diventare un problema, incluso le minacce malware. Allerta truffe monitora tutti i messaggi SMS in arrivo e le notifiche Android in tempo reale.

Quando un link pericoloso arriva in un messaggio sul tuo telefono, sul tuo schermo comparirà un avviso. Bitdefender ti offrirà due opzioni. La prima è ignorare le informazioni, mentre la seconda è **MOSTRA DETTAGLI**. Ciò ti fornisce maggiori informazioni sull'incidente, oltre a consigli essenziali, come:

- Non aprire o inoltrare il link rilevato.
- Per i messaggi di testo, se possibile, eliminali.
- Blocca il mittente se non è un contatto affidabile.
- Elimina la app che invia link pericolosi nelle notifiche.





### Nota

A causa di alcune limitazioni del sistema operativo Android, Bitdefender non può eliminare i messaggi di testo, adottare misure dirette relative ai messaggi SMS o a qualsiasi altra fonte di notifiche dannose. Se ignori l'avviso di Allerta truffe e provi ad aprire il link pericoloso, la funzionalità Protezione web di Bitdefender lo bloccherà, impedendo l'infezione del tuo dispositivo.

### 3.4.1. Attivare Allerta truffe

Per attivare Allerta truffe, devi garantire alla app Bitdefender Mobile Security l'accesso ai messaggi SMS e al sistema di notifica:

1. Apri la app Bitdefender Mobile Security installata sul tuo telefono o tablet Android.
2. Nella schermata principale della app Bitdefender, tocca l'opzione **Allerta truffe** nella barra di navigazione in basso e premi **ATTIVA**.
3. Tocca il pulsante **CONSENTI**.
4. Nell'elenco Accesso alla notifica, imposta Bitdefender Security in posizione **ATTIVA**.
5. Conferma l'azione premendo **CONSENTI**.
6. Torna alla schermata di Allerta truffe e premi **CONSENTI** per garantire a Bitdefender la possibilità di esaminare i messaggi SMS.

### 3.4.2. Protezione chat in tempo reale

I messaggi in chat sono il nostro mezzo più comodo per restare in contatto, ma sono anche un modo semplice con cui i link pericolosi possono raggiungerti.

Con la funzionalità Protezione chat attiva, il modulo Allerta truffe si estende dalla protezione dei messaggi e delle notifiche alla protezione delle chat anche dagli attacchi basati sui link, rilevando i link pericolosi che invii o ricevi mentre chatti.

Per attivare Protezione chat:

1. Apri l'app Bitdefender Mobile Security installata sul tuo telefono o tablet Android.



2. Nella schermata principale della app Bitdefender, tocca l'opzione **Allerta truffe** nella barra di navigazione in basso.
3. Nella parte superiore della scheda Allerta truffe troverai la funzionalità Protezione chat. Imposta l'interruttore corrispondente sulla posizione **ATTIVA**.



### Nota

Attualmente, Protezione chat è compatibile con le seguenti applicazioni:

- WhatsApp
- Facebook Messenger
- Telegram
- Discord

## 3.5. Funzioni Antifurto

Bitdefender può aiutarti a localizzare il tuo dispositivo e impedire che i tuoi dati personali finiscano nelle mani sbagliate.

Tutto ciò che devi fare è attivare Anti-Theft dal dispositivo e, quando necessario, accedere a **Bitdefender Central** da un qualsiasi browser web, ovunque ti trovi.



### Nota

L'interfaccia di Anti-Theft include anche un link alla app Bitdefender Central su Google Play Store. Puoi utilizzarlo per scaricare la app, nel caso non lo avessi già fatto.

Bitdefender Mobile Security offre le seguenti funzionalità Anti-Theft:

### Localizzazione remota

Scopri la posizione attuale del tuo dispositivo su Google Maps. La posizione è aggiornata ogni 5 secondi, in modo da poterlo rintracciare, se è in movimento.

L'accuratezza della posizione dipende da come Bitdefender può rilevarla:

- Se nel dispositivo il GPS è attivato, la sua posizione può essere determinata con un'accuratezza di un paio di metri, finché resta nel raggio dei satelliti GPS (ad esempio, non dentro a un edificio).





- Se il dispositivo è in un edificio, la sua posizione può essere determinata entro decine di metri, se il Wi-Fi è attivato e ci sono reti wireless disponibili nel suo raggio d'azione.
- Diversamente, la posizione sarà determinata usando solo le informazioni dalla rete mobile, che offrono un'accuratezza non superiore a diverse centinaia di metri.

### **Blocco remoto**

Blocca lo schermo del dispositivo e imposta un codice PIN per sbloccarlo.

### **Cancellazione remota**

Rimuovi tutti i dati personali dal dispositivo che hai smarrito.

### **Invia avviso al dispositivo (Allarme)**

Invia un messaggio in remoto che comparirà sullo schermo del dispositivo oppure fallo suonare.



Se perdi il dispositivo, puoi indicare a chi lo trova come restituirlo, facendo comparire un messaggio sul suo schermo.

Se hai smarrito il tuo dispositivo e probabilmente non è molto lontano (ad esempio, da qualche parte in casa o in ufficio), quale modo migliore di ritrovarlo, se non farlo suonare? Il dispositivo emetterà un suono, anche se è in modalità silenziosa.

## 3.5.1. Attivare Anti-Theft

Per attivare le funzioni di Anti-Theft, completa semplicemente la fase di configurazione dalla scheda Anti-Theft, disponibile nell'interfaccia.

In alternativa, puoi attivare Anti-Theft seguendo questi passaggi:

1. Rubinetto  **Di più** nella barra di navigazione in basso.
2. Tocca  **Anti-Theft**.
3. Tocca **ATTIVA**.
4. Per aiutarti ad attivare questa funzione, sarà attivata la seguente procedura:



### Nota

In Android 6, la funzione Anti-Theft richiede alcuni permessi aggiuntivi.

Per attivare l'opzione, segui questi passaggi:

- a. Tocca **Attiva Anti-Theft** e poi **ATTIVA**.
- b. Consenti all'**Antivirus** di accedere alla posizione del tuo dispositivo.

#### a. **Dai privilegi di amministratore**

Questi privilegi sono essenziali per il funzionamento del modulo Anti-Theft e per continuare è necessario assegnarli.

#### b. **Imposta PIN applicazione**

Per impedire l'accesso non autorizzato al tuo dispositivo, occorre impostare un codice PIN. A ogni tentativo di accesso, sarà necessario inserire il PIN. In alternativa, su dispositivi che supportano l'autenticazione tramite impronte digitali, potrà essere utilizzata una conferma tramite impronta digitale invece del codice PIN configurato.

Lo stesso codice PIN viene usato da Blocco App per proteggere le tue applicazioni installate.

#### c. **Attiva Scatta foto**

Ogni volta che qualcuno tenta di sbloccare il tuo dispositivo senza successo con l'opzione Scatta foto attiva, Bitdefender gli scatterà una foto.

Più precisamente, ogni volta che si sbaglia per tre volte di fila a digitare il codice PIN o la password o a confermare l'impronta digitale impostati per proteggere la app, la fotocamera frontale scatta una foto. La foto viene salvata con tanto di indicazione e ora e può essere vista quando si apre Bitdefender Mobile Security e si accede alla finestra di Anti-Theft.

In alternativa, puoi visualizzare la foto scattata nel tuo account di Bitdefender:

- i. Vai a: <https://central.bitdefender.com>.
- ii. Accedi al tuo account.
- iii. Seleziona il **I miei dispositivi** pannello.



- iv. Seleziona il tuo dispositivo Android, quindi la scheda **Anti-Theft**.
- v. Tocca ⓘ accanto a **Controlla i tuoi scatti** per vedere le foto più recenti che sono state scattate.  
Vengono salvate solo le due foto più recenti.

Una volta attivata la funzionalità Anti-Theft, puoi attivare o disattivare i comandi del Controllo web individualmente dalla finestra Anti-Theft toccando le opzioni corrispondenti.




### 3.5.2. Utilizzare le funzioni Anti-Theft da Bitdefender Central



#### Nota

Tutte le funzioni di Anti-Theft richiedono che l'opzione **Dati in background** sia attivata nelle impostazioni di utilizzo dei dati del dispositivo.

Per accedere alle funzionalità di Anti-Theft dal tuo account di Bitdefender:

1. Accedi a **Bitdefender Central**.
2. Seleziona il **I miei dispositivi** pannello.
3. Nella finestra **I MIEI DISPOSITIVI**, seleziona la scheda del dispositivo desiderata toccando il corrispondente pulsante **Mostra dettagli**.
4. Seleziona la scheda **Anti-Theft**.
5. Tocca il pulsante corrispondente della funzionalità che vuoi usare:
  - Localizza** - Mostra la posizione del dispositivo su Google Maps.
  - Mostra IP** - Mostra l'ultimo indirizzo IP per il dispositivo selezionato.
  -  **Allerta** - Digita un messaggio da far comparire sul dispositivo e/o far suonare un allarme.
  -  **Blocca** - Blocca il tuo dispositivo e imposta un codice PIN per sbloccarlo.
  -  **Elimina** - Elimina tutti i dati dal tuo dispositivo.



#### Importante

Dopo aver cancellato il contenuto di un dispositivo, tutte le funzioni di Anti-Theft cessano di funzionare.



### 3.5.3. Impostazioni Anti-Theft

Se desideri attivare o disattivare i comandi remoti:

1. Rubinetto ❄️ **Di più** sulla barra di navigazione in basso.
2. Rubinetto 📍 **Antifurto**.
3. Attiva o disattiva le opzioni desiderate.

### 3.6. Privacy dell'account

Bitdefender Account Privacy rileva se una qualche violazione dei dati si è verificata negli account che utilizzi per effettuare pagamenti e acquisti online, o accedere a diverse app o siti web. I dati memorizzabili in un account possono essere password, informazioni sulle carte di credito o sul conto bancario. Se non protette correttamente, potrebbero verificarsi un furto d'identità o un'invasione alla privacy.

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

Vengono impostati nuovi controlli automatici in background, ma è anche possibile eseguire scansioni manuali su base giornaliera.

Le notifiche saranno mostrate ogni volta che vengono scoperte nuove violazioni che includono uno degli account e-mail verificati.

Per iniziare a proteggere le informazioni personali:

1. Rubinetto ❄️ **Di più** sulla barra di navigazione in basso.
2. Tocca ❄️ **Privacy dell'account**.
3. Tocca **COME INIZIARE**.
4. Comparirà l'indirizzo e-mail utilizzato per creare il tuo account di Bitdefender e sarà aggiunto automaticamente all'elenco degli account monitorati.
5. Per aggiungere un altro account, tocca **AGGIUNGI ACCOUNT** nella finestra Privacy account e poi inserisci l'indirizzo e-mail.  
Tocca **AGGIUNGI** per continuare.  
Bitdefender deve confermare questo account prima di mostrare informazioni private. Inoltre, viene inviata un'e-mail con un codice di conferma all'indirizzo fornito.





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 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 violazioni rilevate come Risolto. Per farlo:

1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Privacy dell'account**.
3. Tocca l'account che hai appena protetto.
4. Tocca la violazione da cui hai protetto l'account.
5. Tocca **RISOLTO** per confermare che l'account è protetto.

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.

Per smettere di essere avvisati ogni volta che vengono eseguite scansioni automatiche:

1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.
3. Disattiva l'interruttore corrispondente nell'area Privacy account.

### 3.7. Blocco App

Le applicazioni installate, così come e-mail, foto o messaggi, possono includere dati personali che si desidera mantenere privati, limitando l'accesso ad essi in modo selettivo.





Blocco App consente di bloccare l'accesso non autorizzato alle applicazioni, impostando un codice di accesso PIN. Il codice PIN impostato deve essere di almeno 4 cifre ma non più lungo di 8, ed è richiesto ogni volta che si vuole accedere alle applicazioni con restrizioni selezionate.

Al posto del codice PIN configurato, è possibile utilizzare l'autenticazione biometrica (come la conferma tramite impronte digitali o riconoscimento facciale).

### 3.7.1. Attivare Blocco App

Per limitare l'accesso alle applicazioni selezionate, configura Blocco App dalla scheda visualizzata nell'interfaccia, dopo aver attivato l'Anti-Theft.

In alternativa, puoi attivare Blocco App seguendo questi passaggi:

1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Tocca  **Blocco App**.
3. Rubinetto **ACCENDERE**.
4. Consenti l'accesso all'utilizzo dei dati per Bitdefender Security.
5. Consenti **trascinamento su altre app**.
6. Torna alla app, configura il codice d'accesso e poi tocca **IMPOSTA PIN**.



#### Nota

Questo passaggio è disponibile solo se non hai configurato in precedenza il PIN in Anti-Theft.

7. Attiva l'opzione Scatta foto per catturare un'immagine di chiunque cercherà di accedere ai tuoi dati privati.



#### Nota

In Android 6, per la funzione Scatta foto sono richiesti alcuni permessi aggiuntivi. Per attivarla, consenti all'**Antivirus** di scattare foto e registrare video.

8. Seleziona le app che vuoi proteggere.



Utilizzando un PIN o un'impronta digitale errata per cinque volte di fila, si attiverà una sessione di tempo massimo consentito di 30 secondi. In questo modo, sarà bloccato ogni tentativo di accedere alle app protette.



### Nota

Lo stesso codice PIN viene usato da Anti-Theft per aiutarti a localizzare il tuo dispositivo.



#### Set Application PIN

Set an application PIN to prevent unauthorized access to your device and apps. Also used by Anti-Theft.

Enter PIN (4-8 digits) 

NOT NOW

SET PIN



## 3.7.2. Modalità Blocco

La prima volta che aggiungi una app a Blocco App, compare la schermata della modalità Blocco App. Qui puoi scegliere quando la funzione Blocco App deve proteggere le app installate sul tuo dispositivo.

Puoi selezionare una delle seguenti opzioni:

- **Richiede uno sblocco ogni volta** - Ogni volta che si accede alle app bloccate, dovrà essere utilizzato il codice PIN o l'impronta digitale impostati.
- **Mantieni sbloccato fino allo spegnimento dello schermo** - L'accesso alle tue app sarà valido fino a quando lo schermo non si spegnerà.
- **Blocca dopo 30 secondi** - Puoi uscire e accedere di nuovo alle app sbloccate entro 30 secondi.

Se vuoi cambiare l'impostazione selezionata:



1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.
3. Tocca **Richiede uno sblocco ogni volta** nell'area Blocco App.



4. Scegli l'opzione desiderata.

### 3.7.3. Impostazioni Blocco App

Per una configurazione avanzata di Blocco App:

1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.

Nell'area Blocco App, puoi configurare le seguenti opzioni:

- Suggerimento app sensibile** - Ricevi una notifica di blocco ogni volta che hai installato una app sensibile.
- Richiede una sblocco ogni volta** - Scegli una delle opzioni di blocco e sblocco disponibili.
- Sblocco rapido** - Mantieni le app sbloccate finché sei connesso a una rete Wi-Fi affidabile.
- Tastiera casuale** - Impedisce la lettura del PIN rendendo casuale le posizioni dei numeri.

### 3.7.4. Scatta foto

Con Bitdefender Snap Photo puoi cogliere sul fatto amici o familiari, evitando che i loro occhi curiosi sbircino i tuoi file personali o le app che utilizzi.



Il suo funzionamento è davvero semplice: ogni volta che si sbaglia per tre volte di fila a digitare il codice PIN o a confermare l'impronta digitale impostati per proteggere la app, la fotocamera frontale scatta una foto. La foto viene salvata con tanto di indicazione e ora e può essere vista quando si apre Bitdefender Mobile Security e si accede alla funzione Blocco App.



#### Nota

Questa funzionalità è disponibile solo per telefoni dotati di una fotocamera frontale.

Per configurare la funzione Scatta foto di Blocco App:


1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.
3. Attiva l'interruttore corrispondente nell'area Scatta foto.







Le foto scattate in caso di inserimento di un PIN errato sono mostrate nella finestra di Blocco App e possono essere visualizzate a schermo intero.

In alternativa, possono essere visualizzate nel tuo account di Bitdefender:

1. Vai a: <https://central.bitdefender.com>.
2. Accedi al tuo account.
3. Seleziona la scheda **Il mio dispositivo**.
4. Seleziona il tuo dispositivo Android, quindi il file **Antifurto** scheda.
5. Rubinetto  accanto a **Controlla le tue istantanee** per visualizzare le ultime foto scattate.

Vengono salvate solo le due foto più recenti.

Per fermare l'invio delle foto scattate sul tuo account Bitdefender:




1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.
3. Disattiva **Carica foto** nell'area Scatta foto.

### 3.7.5. Sblocco rapido

Per evitare che la funzione Blocco App richieda l'inserimento del codice PIN o la conferma dell'impronta digitale per le app protette ogni volta che si accede, basta attivare Sblocco rapido.

Con Sblocco rapido, puoi impostare come affidabili le reti Wi-Fi a cui ti connetti di solito e ogni volta che le userai, le impostazioni di blocco di Blocco App saranno disattivate per le app protette.

Per configurare la funzione Sblocco rapido:

1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Blocco app**.
3. Tocca il pulsante .
4. Tocca l'interruttore accanto a **Sblocca rapido**, se la funzionalità non è ancora stata attivata.

Convalida usando la tua impronta digitale o il tuo PIN.



La prima volta che attiverai la funzionalità, dovrai attivare le autorizzazioni locali. Tocca il pulsante **CONSENTI** e poi tocca ancora **CONSENTI**.

5. Tocca **AGGIUNGI** per impostare come affidabile la connessione Wi-Fi attualmente usata.



Nel caso si cambiasse idea, basterà disattivare la funzione e le reti Wi-Fi impostate come affidabili saranno trattate come se non lo fossero.

### 3.8. Rapporti

Nei Rapporti, è possibile trovare un registro dettagliato degli eventi inerenti le attività di scansione sul proprio dispositivo.

Ogni volta che si verifica qualcosa di rilevante per la sicurezza del dispositivo, un nuovo messaggio viene aggiunto ai Rapporti.

Per accedere alla sezione Rapporti:



1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Tocca  **Rapporti**.

Nella finestra Rapporti, sono disponibili le seguenti schede:

- **RAPPORTI SETTIMANALI** - Qui puoi accedere allo stato della protezione e le attività eseguite nella settimana attuale e in quella precedente. Il rapporto della settimana attuale viene generato ogni domenica e riceverai una notifica ogni volta che sarà disponibile.

In questa sezione, ogni settimana troverai un nuovo suggerimento, perciò assicurati di visitarla regolarmente per sfruttare al massimo la tua app.

Per non ricevere più notifiche ogni volta che viene generato un rapporto:

1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.
3. Disattiva l'interruttore **Notifica nuovo rapporto** nell'area Rapporti.

- **RAPPORTO ATTIVITÀ** - Qui puoi verificare maggiori informazioni sulle attività della tua app Bitdefender Mobile Security da quando è stata installata sul tuo dispositivo Android.

Per eliminare il rapporto attività disponibile:



1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Impostazioni**.
3. Tocca **Cancella rapporto attività** e tocca **AZZERA**.

### 3.9. WearON

Con Bitdefender WearON, puoi localizzare facilmente il tuo smartphone sia che tu l'abbia lasciato in una sala riunioni dell'ufficio o sotto il cuscino del divano. Il dispositivo può essere localizzato persino se era attivata la modalità silenziosa.

Mantieni questa funzione attivata per assicurarti di avere il tuo smartphone sempre a portata di mano.



#### Nota

La funzione richiede Android 4.3 e Android Wear.

#### 3.9.1. Attivare WearON

Per usare WearON, devi solo connettere il tuo smartwatch all'applicazione Bitdefender Mobile Security e attivare la funzione con il seguente comando vocale:

Inizia:<Dov'è il mio telefono>

**Bitdefender WearON** ha due comandi:

##### 1. **Phone Alert**

Con la funzione Phone Alert, puoi trovare rapidamente il tuo smartphone ogni volta che ti allontani troppo da lui.

Se hai il tuo smartwatch con te, rileverà automaticamente la app sul tuo telefono vibrando ogni volta che sarà troppo distante e i dispositivi perderanno la connessione Bluetooth.

Per attivare questa funzione, apri Bitdefender Mobile Security, tocca **Impostazioni generali** nel menu e seleziona l'interruttore corrispondente sotto la sezione WearON.



##### 2. **Allarme**

Trovare il tuo telefono non è mai stato così semplice. Ogni volta che hai dimenticato dove l'hai lasciato, tocca il comando Allarme sul tuo orologio, per far emettere un suono al tuo telefono.



## 3.10. Info

Per trovare informazioni sulla versione di Bitdefender Mobile Security che hai installato, accedere e consultare l'Accordo di abbonamento e l'Informativa sulla privacy, e visualizzare le licenze open source:

1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.
3. Tocca l'opzione desiderata nell'area Informazioni.



## 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 for Android
  - Bitdefender Mobile Security for iOS
  - La linea di prodotti Windows di Bitdefender
  - Bitdefender Antivirus for Mac
- Gestire e rinnovare i tuoi abbonamenti Bitdefender.
- Aggiungi nuovi dispositivi alla tua rete e gestiscili ovunque ti trovi.
- Proteggi i dispositivi nella rete e i loro dati da perdite o furti con la funzione [Anti-Theft](#).

### 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 a: <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. Rubinetto **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 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  $\vdots$  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  $\vdots$  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

### **Perché Bitdefender Mobile Security richiede una connessione a Internet?**



L'applicazione deve comunicare con i server di Bitdefender per determinare lo stato della sicurezza delle applicazioni che controlla e delle pagine web visitate, ma anche per ricevere comandi dal tuo account Bitdefender, quando si utilizzano le funzioni Anti-Theft.

### **Per quali funzioni Bitdefender Mobile Security richiede un'autorizzazione?**

- Accesso a Internet -> Usata per la comunicazione cloud.
- Valutazione dello stato del telefono e dell'identità -> Usata per rilevare se il dispositivo è connesso a Internet e per estrapolare determinate informazioni necessarie a creare un ID univoco per comunicare con il cloud di Bitdefender.
- Lettura e scrittura segnalibri del browser -> Il modulo Protezione web elimina i siti dannosi dalla cronologia.
- Lettura dati del registro -> Bitdefender Mobile Security rileva tracce di attività delle minacce dai registri di Android.
- Posizione -> Richiesta per la localizzazione remota.
- Fotocamera -> Richiesta per Scatta foto.
- Memoria -> Usata per consentire a Scansione malware di esaminare la scheda SD.

### **Come posso smettere di inviare a Bitdefender informazioni sulle app sospette?**



Di norma, Bitdefender Mobile Security invia rapporti ai server di Bitdefender su app sospette che stai installando. Queste informazioni sono essenziali per migliorare il rilevamento delle minacce e possono aiutarci a offrirti un'esperienza migliore in futuro. Nel caso volessi arrestare l'invio di tali informazioni su app sospette:

1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.
3. Disattiva il **Rilevamento in-the-cloud** nell'area Scansione malware.




### Dove posso vedere maggiori dettagli sulle attività dell'app?

Bitdefender Mobile Security salva un rapporto di tutte le azioni importanti, i cambiamenti di stato e gli altri messaggi critici relativi alle sue attività. Per accedere e visualizzare le attività della app:



1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Rapporti**.  
Nella finestra RAPPORTI SETTIMANALI puoi accedere ai rapporti che vengono generati ogni settimana, mentre nella finestra RAPPORTO ATTIVITÀ puoi visualizzare maggiori informazioni sulle attività della tua app di Bitdefender.

### Ho dimenticato il codice PIN impostato per proteggere la mia applicazione. Che cosa posso fare?

1. Accesso [Bitdefender centrale](#).
2. Seleziona il **I miei dispositivi** pannello.
3. Tocca la scheda del dispositivo desiderato e poi tocca  nell'angolo in alto a destra dello schermo.
4. Selezionare **Impostazioni**.
5. Recupera il codice PIN dal campo **PIN per l'applicazione**.

### Come posso modificare il codice PIN impostato per Blocco App e Anti-Theft?

Se desideri modificare il codice PIN impostato per Blocco App e Anti-Theft:

1. Rubinetto  **Di più** nella barra di navigazione in basso.
2. Rubinetto  **Impostazioni**.
3. Tocca **CODICE PIN** di sicurezza nell'area Anti-Theft.
4. Inserisci il codice PIN attuale.
5. Inserisci il nuovo codice PIN che vuoi impostare.

### Come posso disattivare la funzionalità Blocco App?




Non c'è un'opzione per disattivare direttamente l'opzione Blocco App, ma puoi facilmente disattivarla togliendo la spunta delle caselle accanto alle app, dopo aver confermato il PIN o le impronte digitali impostate.






### Come posso impostare un'altra rete wireless come affidabile?

Per iniziare, devi connettere il tuo dispositivo alla rete wireless che vuoi impostare come affidabile. Poi segui questi passaggi:

1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Rubinetto  **Blocco app**.
3. Tocca  nell'angolo in alto a destra.
4. Tocca **AGGIUNGI** accanto alla rete che vuoi impostare come affidabile.

### Come posso smettere di vedere le fotografie scattate dai miei dispositivi?

Per smettere di rendere visibili le fotografie scattate sui tuoi dispositivi:

1. Accesso [Bitdefender centrale](#).
2. Tocca  in alto a destra dello schermo.
3. Tocca **Impostazioni** nel menu scorrevole.
4. Disattiva l'opzione **Mostra/non mostrare le foto scattate sui tuoi dispositivi**.

### Come posso mantenere sicuri i miei acquisti online?

Quando si ignorano alcuni dettagli, gli acquisti online possono comportare dei rischi elevati. Per non cadere vittima di una frode, ti consigliamo di seguire questi suggerimenti:

- Mantieni la tua app di sicurezza aggiornata.
- Invia pagamenti online solo con la protezione dell'acquirente.
- Usa una VPN quando ti connetti a internet da reti wireless pubbliche e non protette.
- Presta attenzione alle password che hai assegnato ai tuoi account online. Devono essere sicure, includendo sia lettere maiuscole che minuscole, numeri e simboli (@, !, %, #, ecc.).
- Assicurati di inviare le tue informazioni sempre con connessioni sicure. L'estensione del sito web online deve essere HTTPS:// e non HTTP://.

### Quando devo utilizzare Bitdefender VPN?



Devi fare sempre attenzione quando accedi, scarichi o invii contenuti su internet. Per assicurarti di essere sempre al sicuro mentre navighi sul web, ti consigliamo di utilizzare Bitdefender VPN quando:

- vuoi connetterti a reti wireless pubbliche
- vuoi accedere a contenuti che normalmente sono riservati a determinate aree, indipendentemente dal fatto che ti trovi a casa o all'estero
- vuoi mantenere i tuoi dati personali privati (nomi utente, password, informazioni della carta di credito, ecc.)
- vuoi nascondere il tuo indirizzo IP

### **Bitdefender VPN avrà un impatto negativo sulla durata della batteria del mio dispositivo?**


Bitdefender VPN è progettato per proteggere i tuoi dati personali, nascondere il tuo indirizzo IP mentre ti connetti a reti wireless non sicure e accedere a contenuti inaccessibili in determinati paesi. Per evitare un consumo non necessario della batteria del tuo dispositivo, ti consigliamo di utilizzare VPN solo quando ne hai bisogno e disconnetterti quando sei offline.

### **Perché riscontro rallentamenti in Internet durante la connessione con Bitdefender VPN?**

Bitdefender VPN è stato progettato per offrirti un'esperienza di navigazione sul web leggera; tuttavia, la tua connettività a Internet o la distanza del server a cui ti connetti potrebbero causare dei rallentamenti. In questo caso, se non è obbligatorio connetterti a un server ospitato molto distante (ad esempio negli Stati Uniti o in Cina), ti consigliamo di consentire a Bitdefender VPN di connettersi automaticamente al server più vicino o trovarne uno più vicino alla tua ubicazione attuale.

### **Posso cambiare l'account Bitdefender associato al mio dispositivo?**

Sì, puoi facilmente modificare l'account di Bitdefender collegato al tuo dispositivo seguendo questi passaggi:

1. Rubinetto  **Di più** sulla barra di navigazione in basso.
2. Tocca il tuo indirizzo e-mail.
3. Tocca **Esci dal tuo account**. Se è stato impostato un codice PIN, ti sarà chiesto di inserirlo.



4. Conferma la tua scelta.
5. Inserisci l'indirizzo email e la password del tuo account nei campi corrispondenti, e tocca **ACCEDI**.

### **In che modo Bitdefender Mobile Security influenza le prestazioni del dispositivo e l'autonomia della batteria?**

Abbiamo mantenuto un basso impatto sulle prestazioni. L'applicazione si attiva solo quando serve, dopo aver installato un'applicazione, mentre si usa l'interfaccia o si esegue un controllo di sicurezza. Bitdefender Mobile Security non funziona in background mentre chiami gli amici, digiti un messaggio o giochi.

### **Che cos'è la funzione Amministratore dispositivo?**

Amministratore dispositivo è una funzione di Android che dà a Bitdefender Mobile Security le autorizzazioni necessarie per eseguire determinati compiti in remoto. Senza questi privilegi, il Blocco remoto non funzionerebbe e la cancellazione non potrebbe rimuovere completamente i tuoi dati. Se desideri rimuovere l'applicazione, assicurati di revocare tali privilegi prima della disinstallazione, andando in **Impostazioni > Sicurezza > Seleziona Amministratori dispositivo**.

### **Come risolvere l'errore "Nessun token Google" che compare quando ci si registra a Bitdefender Mobile Security.**

Questo errore si verifica quando il dispositivo non è associato a un account Google, oppure se associato, un problema temporaneo impedisce la connessione a Google. Prova una delle seguenti soluzioni:

- Vai in Impostazioni Android > Applicazioni > Gestisci applicazioni > Bitdefender Mobile Security e tocca **Cancella dati**. Poi riprova ad accedere.
- Assicurati che il dispositivo sia associato con un account Google. Per controllare, vai in Impostazioni > Account per poi sincronizzare e verificare se un account Google è indicato sotto la voce **Gestione account**. Se non c'è, riavvia il dispositivo e riprova ad accedere a Bitdefender Mobile Security.
- Riavvia il dispositivo e riprova ad accedere.

### **In quali lingue è disponibile Bitdefender Mobile Security?**

Attualmente, Bitdefender Mobile Security è disponibile nelle seguenti lingue:



- Brasiliano
- Ceco
- Olandese
- Inglese
- Francese
- Tedesco
- Greco
- Ungherese
- Italiano
- Giapponese
- Coreano
- Polacco
- Portoghese
- Romeno
- Russo
- Spagnolo
- Svedese
- Thai
- Turco
- Vietnamita

Altre lingue saranno aggiunte nei futuri aggiornamenti. Per cambiare la lingua dell'interfaccia di Bitdefender Mobile Security, vai alle impostazioni **Lingua e tastiera** del dispositivo e imposta la lingua che vuoi usare.



## 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 \(pagina 49\)](#).

<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 riassettaggio 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.