

USER'S GUIDE

**Bitdefender**<sup>®</sup> CONSUMER  
SOLUTIONS

# Mobile Security





# Bitdefender Mobile Security

## User's Guide

Publication date 10/02/2023  
Copyright © 2023 Bitdefender

## Legal Notice

**All rights reserved.** No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

**Warning and Disclaimer.** This product and its documentation are protected by copyright. The information in this document is provided on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

**Trademarks.** Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.

**Bitdefender®**



# Table of Contents

- About This Guide ..... 1**
  - Purpose and Intended Audience ..... 1
  - How to Use This Guide ..... 1
  - Conventions used in This Guide ..... 1
    - Typographical Conventions ..... 1
    - Admonitions ..... 2
  - Request for Comments ..... 2
- 1. What is Bitdefender Mobile Security ..... 3**
- 2. Getting Started ..... 4**
  - 2.1. Device Requirements ..... 4
  - 2.2. Installing Bitdefender Mobile Security ..... 4
  - 2.3. Sign in to your Bitdefender account ..... 5
  - 2.4. Configure Protection ..... 6
  - 2.5. Dashboard ..... 6
- 3. Features & Functionalities ..... 9**
  - 3.1. Malware Scanner ..... 9
    - 3.1.1. App Anomaly Detection ..... 11
  - 3.2. Web Protection ..... 11
  - 3.3. VPN ..... 13
    - 3.3.1. VPN Settings ..... 14
    - 3.3.2. Subscriptions ..... 15
  - 3.4. Scam Alert ..... 15
    - 3.4.1. Activating Scam Alert ..... 16
    - 3.4.2. Real-time Chat Protection ..... 17
  - 3.5. Anti-Theft Features ..... 17
    - 3.5.1. Activating Anti-Theft ..... 18
    - 3.5.2. Using Anti-Theft features from Bitdefender Central ..... 20
    - 3.5.3. Anti-Theft Settings ..... 20
  - 3.6. Account Privacy ..... 21
  - 3.7. App Lock ..... 22
    - 3.7.1. Activating App Lock ..... 23
    - 3.7.2. Lock mode ..... 24
    - 3.7.3. App Lock Settings ..... 24
    - 3.7.4. Snap Photo ..... 25
    - 3.7.5. Smart Unlock ..... 26
  - 3.8. Reports ..... 26
  - 3.9. WearON ..... 27
    - 3.9.1. Activating WearON ..... 28
  - 3.10. About ..... 28



- 4. Frequently Asked Questions ..... 29
- 5. Getting Help ..... 35
  - 5.1. Asking for Help ..... 35
  - 5.2. Online Resources ..... 35
    - 5.2.1. Bitdefender Support Center ..... 35
    - 5.2.2. The Bitdefender Expert Community ..... 36
    - 5.2.3. Bitdefender Cyberpedia ..... 36
  - 5.3. Contact Information ..... 36
    - 5.3.1. Local distributors ..... 37
- Glossary ..... 38



## ABOUT THIS GUIDE

### Purpose and Intended Audience

This guide is intended to all Android users who have chosen Bitdefender Mobile Security as a security solution for their mobile devices. The information presented in this book is suitable not only for those with a technical background, it is accessible to everyone who is able to work under Android devices.

You will find out how to configure and use Bitdefender Mobile Security to protect yourself against threats and other malicious applications. You will learn how to get best from Bitdefender.

We wish you a pleasant and useful lecture.

### How to Use This Guide

This guide is organized around several major topics:

[Getting Started \(page 4\)](#)

Get started with Bitdefender Mobile Security and its user interface.

[Features & Functionalities \(page 9\)](#)

Learn how to use Bitdefender Mobile Security to protect yourself against threats and malicious applications by learning about its features and their functionalities.

[Getting Help \(page 35\)](#)

Where to look and where to ask for help if something unexpected appears.

## Conventions used in This Guide

### Typographical Conventions

Several text styles are used in this guide for an improved readability. Their aspect and meaning are presented in the table below.



Appearance	Description
sample syntax	Syntax samples are printed with monospaced characters.
<a href="https://www.bitdefender.com">https://www.bitdefender.com</a>	The URL link is pointing to some external location, on http or ftp servers.
<a href="mailto:documentation@bitdefender.com">documentation@bitdefender.com</a>	Email addresses are inserted in the text for contact information.
<a href="#">About this Guide (page 1)</a>	This is an internal link, towards some location inside the document.
filename	File and directories are printed using monospaced font.
<b>option</b>	All the product options are printed using <b>bold</b> characters.
<b>keyword</b>	Important keywords or phrases are highlighted using <b>bold</b> characters.

Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.



Note

The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.



Important

This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.



Warning

This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

Request for Comments

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability. Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you with the best documentation possible.

Let us know by sending an email to [documentation@bitdefender.com](mailto:documentation@bitdefender.com). Write all of your documentation-related emails in English so that we can process them efficiently.



# 1. WHAT IS BITDEFENDER MOBILE SECURITY

Online activities such as paying bills, making holiday reservations, or buying goods and services are convenient and hassle-free. But as many activities evolved on the internet, these come with high risks and, if security details are ignored, personal data may be hacked. And what is more important than protecting data stored in online accounts and on the personal smartphone?

**Bitdefender Mobile Security** allows you to:

- Gain the best protection for your Android smartphone and tablet with minimal impact on battery life
- Protect yourself from falling victim to link-based mobile scams
- Have access to our secure VPN for a fast, anonymous and safe experience while surfing the web
- Remotely locate, lock and wipe your Android device in case of loss or theft
- Verify whether your email account has been involved in data breakages or data leaks



## 2. GETTING STARTED

### 2.1. Device Requirements

Bitdefender Mobile Security works on any device running Android 5.0 or any later versions of the operating system. An active internet connection is required for in-the-cloud threat scanning.

### 2.2. Installing Bitdefender Mobile Security

#### ○ From Bitdefender Central

##### ○ On Android

1. Go to: <https://central.bitdefender.com>.
2. Sign in to your Bitdefender account.
3. Select the **My Devices** panel.
4. Tap **INSTALL PROTECTION**, and then tap **Protect this device**.
5. Select the owner of the device. If the device belongs to someone else, tap the corresponding button.
6. You are redirected to the **Google Play** app. In the Google Play screen, tap the installation option.

##### ○ On Windows, macOS, and iOS

1. Go to: <https://central.bitdefender.com>.
2. Sign in to your Bitdefender account.
3. Select the **My Devices** panel.
4. Press **INSTALL PROTECTION**, and then press **Protect other devices**.
5. Select the owner of the device. If the device belongs to someone else, press the corresponding button.
6. Press **SEND DOWNLOAD LINK**.
7. Type an email address in the corresponding field, and press **SEND EMAIL**. Note that the generated download link is valid



for the next 24 hours only. If the link expires, you will have to generate a new one by following the same steps.

8. On the device you want to install Bitdefender check the email account that you typed in, and then press the corresponding download button.

### ○ From Google Play

Search for Bitdefender Mobile Security to locate and install the app. Alternatively, scan the QR Code:



Before going through the validation steps, you have to agree with the Subscription Agreement. Please take some time to read the Subscription Agreement as it contains the terms and conditions under which you may use Bitdefender Mobile Security.

Tap **CONTINUE** to proceed to the next window.

## 2.3. Sign in to your Bitdefender account

To use Bitdefender Mobile Security, you must link your device to a Bitdefender, Facebook, Google, Microsoft, or Apple account by signing in to the account from the app. The first time you open the app, you will be prompted to sign in to an account.

If you installed Bitdefender Mobile Security from your Bitdefender account, the app will attempt to automatically sign in to that account.

To link your device to a Bitdefender account:

1. Type your Bitdefender account email address and password in the corresponding fields. If you do not have a Bitdefender account and want to create one, select the corresponding link.
2. Tap **SIGN IN**.

To sign in using a Facebook, Google, or Microsoft account, tap the service you want to use from the OR SIGN WITH area. You are redirected to the



login page of the selected service. Follow the instructions to link your account to Bitdefender Mobile Security.



### Note

Bitdefender does not get access to any confidential information such as the password of the account you use to sign in, or the personal information of your friends and contacts.

## 2.4. Configure Protection

Once you successfully sign in to the app, the Configure protection window appears. To secure your device, we recommend you to go through these steps:

- **Subscription status.** To be protected by Bitdefender Mobile Security, you must activate your product with a subscription, which specifies how long you may use the product. As soon as it expires, the app stops performing its functions and protecting your device.  
If you have an activation code, tap **I HAVE A CODE**, and then tap **ACTIVATE**.  
If you have signed in with a new Bitdefender account and have no activation code, you can use the product for 14 days, free of charge.
- **Web Protection.** If your device requires Accessibility to activate Web Protection, tap **ACTIVATE**. You are redirected to the Accessibility menu. Tap Bitdefender Mobile Security, and then turn on the corresponding switch.
- **Malware Scanner.** Run a one-time scan to make sure that your device is free from threats. To initiate the scan process, tap **SCAN NOW**.  
As soon as the scanning process begins, the dashboard appears. Here you can see the security status of your device.

## 2.5. Dashboard

Tap the Bitdefender Mobile Security icon in your device's app drawer to open the app interface.

The Dashboard offers information about the security status of your device and through Autopilot helps you to improve your device security by giving you features recommendations.

The status card at the top of the window informs you about the device's security status using explicit messages and suggestive colors.



If Bitdefender Mobile Security has no warnings, the status card is green. When a security issue has been detected, the status card changes its color into red.

To offer you an effective operation and increased protection while carrying out different activities, **Bitdefender Autopilot** will act as your personal security advisor. Depending on the activity you perform, Bitdefender Autopilot will come up with contextual recommendations based on your device usage and needs. This will help you discover and benefit from the advantages brought by the features included into the Bitdefender Mobile Security app.

Whenever there is a process in progress or a feature requires your input, a card with more information and possible actions is displayed in the Dashboard.

You can access the Bitdefender Mobile Security features and easily navigate from the bottom navigation bar:

### **Malware Scanner**

Allows you to initiate an on-demand scan and enable Scan Storage. For more information, refer to [Malware Scanner \(page 9\)](#).

### **Web Protection**

Ensures a safe browsing experience by alerting you about potential malicious webpages. For more information, refer to [Web Protection \(page 11\)](#).

### **VPN**

Encrypts internet communication, helping you maintain your privacy no matter what network you are connected to. For more information, refer to [VPN \(page 13\)](#).

### **Scam Alert**

Keeps you safe by alerting you of malicious links arriving via SMS, messaging applications and any type of notification. For more information, refer to [Scam Alert \(page 15\)](#).

### **Anti-Theft**

Allows you to turn the Anti-Theft features on or off and to configure Anti-Theft settings. For more information, refer to [Anti-Theft Features \(page 17\)](#).



Account Privacy

Checks if any data breach has occurred in your online accounts. For more information, refer to [Account Privacy \(page 21\)](#).

App Lock

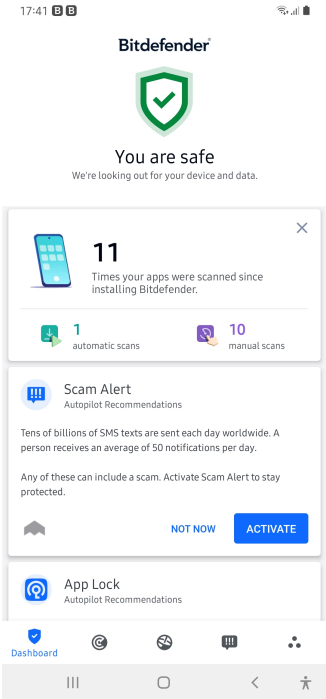
Allows you to protect your installed apps by setting a PIN access code. For more information, refer to [App Lock \(page 22\)](#).

Reports

Keeps a log of all important actions, status changes and other critical messages related to your device ’s activity. For more information, refer to [Reports \(page 26\)](#).

WearON

Communicates with your smartwatch to help you find your phone in case you misplace or forget where you left it. For more information, refer to [WearON \(page 27\)](#).





## 3. FEATURES & FUNCTIONALITIES

### 3.1. Malware Scanner

Bitdefender protects your device and data against malicious apps using on-install scanning and on-demand scanning.

The Malware Scanner interface provides a list of all the types of threats Bitdefender looks for, along with their definitions. Simply tap on any threat to view its definition.



#### Note

Make sure your mobile device is connected to the internet. If your device is not connected to the internet, the scan process will not start.

#### ○ On-install scanning


Whenever you install an app, Bitdefender Mobile Security automatically scans it using in-the-cloud technology. The same scanning process starts each time the installed apps are updated.

If the app is found to be malicious, an alert will appear prompting you to uninstall it. Tap **Uninstall** to go to that app's uninstall screen.

#### ○ On-demand scanning

Whenever you want to make sure that the apps installed on your device are safe to use, you can initiate an on-demand scan.

To start an On-demand scan:

1. Tap  **Malware Scanner** on the bottom navigation bar.
2. Tap **START SCAN**.



#### Note

Additional permissions are required on Android 6 for the Malware Scanner feature. After tapping **START SCAN**, select **Allow** for the following:



- Allow **Antivirus** to make and manage phone calls?
- Allow **Antivirus** to access photos, media, and files on your device?

The scan progress is displayed and you can stop the process at any time.




By default, Bitdefender Mobile Security will scan your device's internal storage, including any mounted SD card. This way, any dangerous apps that might be on the card can be detected before they can cause harm.

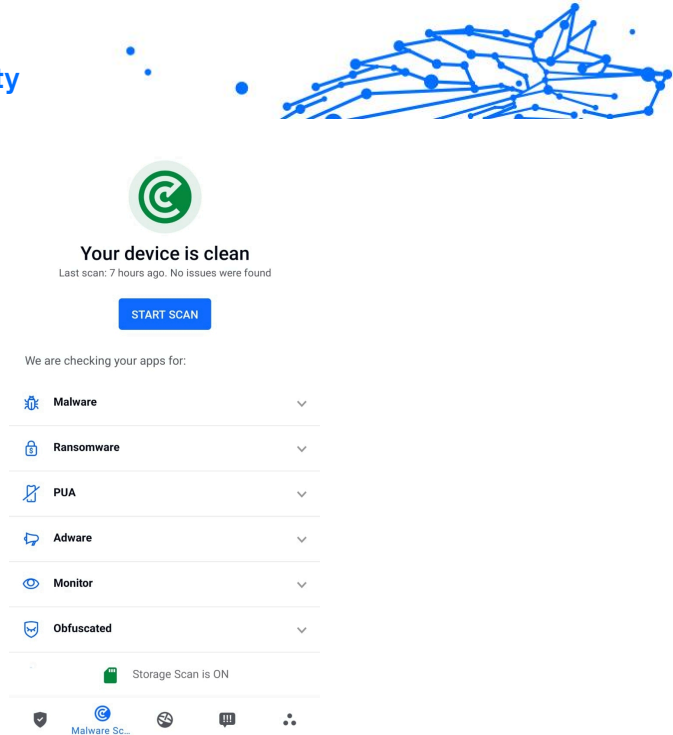
To disable the Scan Storage setting:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.
3. Disable the **Scan Storage** switch in the Malware Scanner area.

If any malicious apps are detected, information about them will be displayed and you can remove them by tapping **UNINSTALL**.

The Malware Scanner card displays the state of your device. When your device is safe, the card is green. When the device requires a scan, or there is any action that requires your input, the card will turn red.

If your Android's version is 7.1 or newer, you can access a shortcut to Malware Scanner so that you can run scans faster, without opening the Bitdefender Mobile Security interface. To do this, press and hold the Bitdefender icon on your Home screen or Apps drawer, and then select the  icon.



### 3.1.1. App Anomaly Detection

Bitdefender App Anomaly Detection is a novel technology integrated into the Bitdefender Malware Scanner to provide an additional layer of protection by continuously monitoring and detecting any malicious behaviors and alerting the user if suspicious activities are identified.

Bitdefender App Anomaly Detection protects users even when they have unknowingly installed a dangerous app that runs dormant for a period of time or a seemingly trusted app that breaks its functionality and turns rogue.

### 3.2. Web Protection

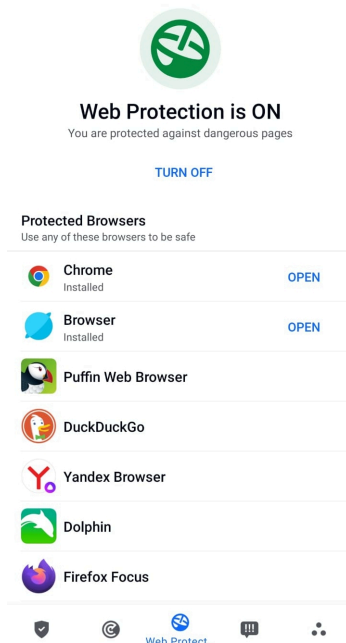
Web Protection checks using Bitdefender cloud services webpages you access with the default Android browser, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser and Dolphin.



### Note



Additional permissions are required on Android 6 for the Web Protection feature.

Allow permission to register as Accessibility service and tap **TURN ON** when requested. Tap **Antivirus** and enable the switch, then confirm that you agree with the access to your device's permission.



Each time you access a banking site, Bitdefender Web Protection is set to notify you to use Bitdefender VPN. The notification appears in the status bar. We recommend you to use Bitdefender VPN while you are signed in into your bank account so that your data can stay safe from potential security breaches.

To disable the Web Protection notification:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.



3. Turn off the corresponding switch in the Web Protection area.

### 3.3. VPN

With Bitdefender VPN you can keep your data private each time you connect to unsecured wireless networks while in airports, malls, cafés, or hotels. This way, unfortunate situations such as theft of personal data, or attempts to make your device's IP address accessible to hackers can be avoided.


The VPN serves as a tunnel between your device and the network you connect to securing your connection, encrypting the data using bank-grade encryption, and hiding your IP address wherever you are. Your traffic is redirected through a separate server; thus making your device almost impossible to be identified through the myriad of other devices that are using our services. Moreover, while connected to the internet via VPN, you are able to access content that is normally restricted in specific areas.



#### Note

Some countries practice internet censorship and therefore the usage of VPNs on their territory has been banned by law. To avoid legal consequences, a warning message can appear when you try to use the Bitdefender VPN app for the first time. By continuing using the app, you confirm that you are aware of the applicable country regulations and the risks to which you might be exposed.

There are two ways to turn on or off Bitdefender VPN:

- Tap **CONNECT** in the VPN card from the Dashboard.  
The status of Bitdefender VPN is displayed.
- Tap  **VPN** on the bottom navigation bar, and then tap **CONNECT**.  
Tap **CONNECT** each time you want to stay protected while connected to unsecured wireless networks.  
Tap **DISCONNECT** whenever you want to disable the connection.




#### Note

The first time you turn on VPN, you are asked to allow Bitdefender to set up a VPN connection that will monitor network traffic. Tap **OK** to continue.

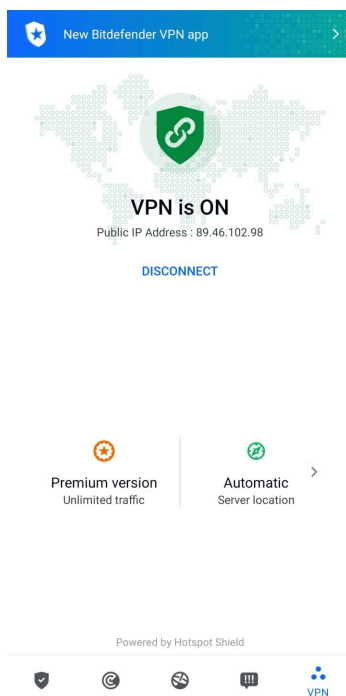


If your Android's version is 7.1 or newer, you can access a shortcut to Bitdefender VPN, without opening the Bitdefender Mobile Security interface.

To do this, press and hold the Bitdefender icon on your Home screen or Apps drawer, and then select the  icon.

To save battery power, we recommend you to turn off the VPN feature when you do not need it.



If you have a premium subscription and would like to connect to a server at your will, tap Server Location in the VPN feature, and then select the location you want. For details about VPN subscriptions, refer to



### 3.3.1. VPN Settings

For an advanced configuration of your VPN:



1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.

In the VPN area, you can configure the following options:

- ☐ Quick VPN access - a notification will appear in the status bar of your device to allow you to quickly turn on VPN.
- ☐ Open Wi-Fi warning - each time you connect to an open Wi-Fi network, you are notified in the status bar of your device to use VPN.

### 3.3.2. Subscriptions

Bitdefender VPN offers for free a daily 200 MB traffic quota per device to secure your connection every time you need, and connects you automatically to the optimal server location.

To get unlimited traffic and unrestricted access to content worldwide by choosing a server location at your will, upgrade to the premium version.

You can upgrade to the Bitdefender Premium VPN version anytime by tapping on **Activate Premium** in the VPN window.

The Bitdefender Premium VPN subscription is independent from the Bitdefender Mobile Security subscription, meaning you will be able to use it for its entire availability, regardless of the state of your security subscription. In case the Bitdefender Premium VPN subscription expires, but the one for Bitdefender Mobile Security is still active, you will be reverted to the free plan.

Bitdefender VPN is a cross-platform product, available in the Bitdefender products compatible with Windows, macOS, Android, and iOS. Once you upgrade to the premium plan, you will be able to use your subscription on all products, provided that you login with the same Bitdefender account.



#### Note

Bitdefender VPN also works as a standalone application on all supported operating systems, namely Windows, macOS, Android and iOS.

### 3.4. Scam Alert

The Scam Alert feature takes preventive measures to the forefront, dealing with potentially dangerous situations before they even have a



chance to become a problem, including malware threats. Scam Alert monitors all incoming SMS messages and Android notifications in real-time.

When a dangerous link arrives in a message on your phone, a warning will pop up on your screen. Bitdefender will offer two options. The first option is to dismiss the information. The second option is to **VIEW DETAILS**. This provides you with more information about the incident, as well as essential pieces of advice, such as:

- Don't open or forward the detected link.
- For texts, delete the message if possible.
- Block the sender if they're not a trusted contact.
- Uninstall the app that sends dangerous links in notifications.



### Note

Due to Android operating system limitations, Bitdefender cannot delete text messages, take any direct measures related to the SMS messages, or any other source of malicious notifications. If you ignore the Scam Alert warning and try to open the dangerous link, Bitdefender's Web Protection feature will automatically catch it, preventing your device from becoming infected.

### 3.4.1. Activating Scam Alert

To enable Scam Alert, you need to grant the Bitdefender Mobile Security app access to the SMS messages and the notification system:

1. Open the Bitdefender Mobile Security app installed on your Android phone or tablet.
2. In the Bitdefender app main screen, tap the **Scam Alert** option on the bottom navigation bar, then press **TURN ON**.
3. Tap the **ALLOW** button.
4. In the Notification Access list, toggle Bitdefender Security to the **ON** position.
5. Confirm the action by pressing **ALLOW**.
6. Return to the Scam Alert screen and press **ALLOW** to give Bitdefender the ability to scan incoming SMS messages.



### 3.4.2. Real-time Chat Protection

Chat messages are our most comfortable mean of keeping in touch, but they're also an easy way for dangerous links to reach you.

With the Chat Protection feature active, the Scam Alert module is extended from protecting your texts and notifications to keeping your chats safe against link-based attacks as well, by detecting dangerous links you either send or receive while chatting.

To enable Chat Protection:

1. Open the Bitdefender Mobile Security app installed on your Android phone or tablet.
2. In the Bitdefender app main screen, tap the **Scam Alert** option on the bottom navigation bar.
3. You will be met by the Chat Protection feature at the top of the Scam Alert tab. Toggle its corresponding switch to the **ON** position.



#### Note

Currently, Chat Protection is compatible with the following applications:

- ☐ WhatsApp
- ☐ Facebook Messenger
- ☐ Telegram
- ☐ Discord

### 3.5. Anti-Theft Features

Bitdefender can help you locate your device and prevent your personal data from getting into the wrong hands.

All you need to do is activate Anti-Theft from the device and, when needed, access **Bitdefender Central** from any web browser, anywhere.



#### Note

The Anti-Theft interface also includes a link to our Bitdefender Central app on Google Play Store. You can use this link to download the app, in case you haven't done it already.

Bitdefender Mobile Security offers the following Anti-Theft features:

#### Remote Locate



View your device's current location on Google Maps. The location is refreshed every 5 seconds, so you can track it if it is on the move.

The accuracy of the location depends on how Bitdefender is able to determine it:

- If the GPS is enabled on the device, its location can be pinpointed to within a couple of meters as long it is in the range of GPS satellites (i.e. not inside a building).
- If the device is indoors, its location can be determined to within tens of meters if Wi-Fi is enabled and there are wireless networks available in its range.
- Otherwise, the location will be determined using only information from the mobile network, which can offer an accuracy no better than several hundred meters.

### **Remote Lock**

Lock your device's screen and set a numeric PIN for unlocking it.

### **Remote Wipe**

Remove all personal data from your estranged device.

### **Send alert to device (Scream)**

Remotely send a message to be displayed on the device's screen, or trigger a loud sound to be played on the device speaker.


If you lose your device, you can let whoever finds it know how they can return it to you by displaying a message on the screen of the device.

If you misplaced your device and there is a chance it is not far from you (for example, somewhere around the house or the office), what better way to find it than to make it play a loud sound? The sound will be played even if the device is in silent mode.


## 3.5.1. Activating Anti-Theft

To enable Anti-Theft features, simply complete the configuration process from the Anti-Theft card available in the Dashboard.

Alternatively, you can activate Anti-Theft by following these steps:

1. Tap  **More** on the bottom navigation bar.



2. Tap  **Anti-Theft**.
3. Tap **TURN ON**.
4. The following procedure will begin to help you activate this feature:



### Note

Additional permissions are required on Android 6 for the Anti-Theft feature.

To enable it, follow these steps:

- a. Tap **Activate Anti-Theft**, then tap **TURN ON**.
  - b. Allow permissions for **Antivirus** to access your device's location.
- a. **Grant Admin Privileges**

These privileges are essential to the operation of Anti-Theft and therefore must be granted to continue.
- b. **Set Application PIN**

To prevent unauthorized access to your device, a PIN code must be set. Every time an attempt will be made to access your device, the PIN will have to be entered first. Alternatively, on devices that support fingerprint authentication, a fingerprint confirmation can be used instead of the configured PIN code.


The same PIN code is used by App Lock to protect your installed apps.
- c. **Activate Snap Photo**

Each time someone will try to unlock your device without success while Snap Photo is turned on, Bitdefender will take a photo of him. More exactly, every time the PIN code, password, or fingerprint confirmation you set to protect your device is entered wrong three times in a row, a photo is taken using the front camera. The photo is saved together with the time-stamp and reason, and can be seen when you open Bitdefender Mobile Security and access the Anti-Theft window.

Alternatively, you can view the taken photo in your Bitdefender account:

  - i. Go to: <https://central.bitdefender.com>.
  - ii. Sign in to your account.



- iii. Select the **My Devices** panel.
- iv. Select your Android device, and then the **Anti-Theft** tab.
- v. Tap  next to **Check your snapshots** to view the latest photos that were taken.  
Only the two most recent photos are saved.

Once the Anti-Theft feature is activated, you can enable or disable Web Control commands individually from the Anti-Theft window by tapping the corresponding options.




### 3.5.2. Using Anti-Theft features from Bitdefender Central



#### Note

All Anti-Theft features require the **Background data** option to be enabled in your device's Data usage settings.

To access the Anti-Theft features from your Bitdefender account:

1. Access [Bitdefender Central](#).
2. Select the **My Devices** panel.
3. In the **MY DEVICES** window, select the desired device card by tapping on its corresponding **View details** button.
4. Select the **Anti-Theft** tab.
5. Tap the button corresponding to the feature you want to use:
  - Locate** - display your device's location on Google Maps.
  - SHOW IP** - displays the last IP address for the selected device.
  -  **Alert** - type a message to display on your device's screen and/or make your device play a sound alarm.
  -  **Lock** - lock your device and set a PIN code for unlocking it.
  -  **Wipe** - delete all data from your device.





#### Important

After you wipe a device, all Anti-Theft features cease to function.

### 3.5.3. Anti-Theft Settings

If you wish to enable or disable the remote commands:



1. Tap  **More** on the bottom navigation bar.
2. Tap  **Anti-Theft**.
3. Enable or disable the desired options.

### 3.6. Account Privacy



Bitdefender Account Privacy detects if any data breach has occurred in the accounts you use for making online payments, shopping, or signing in different apps or websites. The data that may be stored into an account can be passwords, credit card information, or bank account information, and, if not properly secured, identity theft or invasion to privacy may occur.

The privacy status of an account is displayed right after validation.

Automatic rechecks are set to run in the background, but manual scans can be run as well on a daily basis.

Notifications will be displayed each time new breaches that include any of the validated email accounts are discovered.

To start keeping personal information safe:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Account Privacy**.
3. Tap **GET STARTED**.
4. The email address used to create your Bitdefender account appears and is automatically added to the list of monitored accounts.
5. To add another account, tap **ADD ACCOUNT** in the Account Privacy window, and then type the e-mail address.

Tap **ADD** to continue.

Bitdefender needs to validate this account before displaying private information. Therefore, an email with a validation code is sent to the provided email address.

Check your inbox, and then type the received code in the **Account Privacy** area of your app. If you cannot find the validation email in the Inbox folder, check the Spam folder.



The privacy status of the validated account is displayed.



If breaches are found in any of your accounts, we recommend you to change their password as soon as possible. To create a strong and secure password, take into consideration these tips:



- Make it at least eight characters long.
- Include lower and upper case characters.
- Add at least one number or symbol, such as #, @, % or !.

Once you secured an account that was part of a privacy breach, you can confirm the changes by marking the identified breach(es) as Solved. To do this:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Account Privacy**.
3. Tap the account you just secured.
4. Tap the breach you secured the account for.
5. Tap **SOLVED** to acknowledge that the account is secured.

When all the detected breaches are marked as **Solved**, the account will no longer appear as breached, at least until a new breach is detected.

To stop being notified each time automatic scans are done:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.
3. Turn off the corresponding switch in the Account Privacy area.

### 3.7. App Lock

Installed apps such as emails, photos, or messages, can contain personal data that you would like to remain private by selectively restricting access to them.

App Lock helps you block unwanted access to apps by setting a security PIN access code. The PIN code you set must be at least 4 digits long, but not more than 8, and is required every time you want to access the selected restricted apps.

Biometric authentication (such as fingerprint confirmation or face recognition) can be used instead of the configured PIN code.



### 3.7.1. Activating App Lock

To restrict access to selected apps, configure App Lock from the card displayed in the Dashboard after activating Anti-Theft.

Alternatively, you can activate App Lock by following these steps:

1. Tap **More** on the bottom navigation bar.
2. Tap **App Lock**.
3. Tap **TURN ON**.
4. Allow access to usage data for Bitdefender Security.
5. Allow **draw over other apps**.
6. Go back to the app, configure the access code, and then tap **SET PIN**.



#### Note

This step is available only if you didn't previously configure the PIN in Anti-Theft.

7. Enable the Snap Photo option to catch any intruder that will try to access your private data.



#### Note

Additional permissions are required on Android 6 for the Snap Photo feature. To enable it, allow **Antivirus** to take pictures and record video.

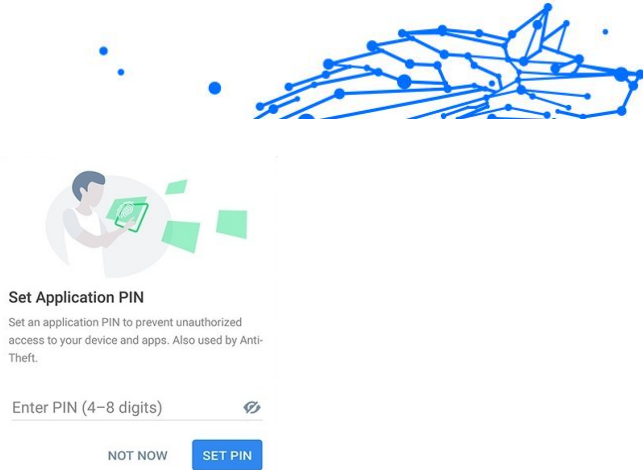
8. Select the apps you want to protect.

Using the wrong PIN or fingerprint five times in a row, will activate a 30 seconds time-out session. This way, any attempt to break in the protected apps will be blocked.



#### Note

The same PIN code is used by Anti-Theft to help you locate your device.





### 3.7.2. Lock mode

The first time you add an app to App Lock, the App Lock Mode screen appears. From here you can choose when the App Lock feature should protect the apps installed on your device.

You can choose from one of the following options:



- **Require unlock every time** - each time the locked apps are accessed, the PIN code or fingerprint you have set up will have to be used.
- **Keep unlocked until screen off** - the access to your apps will be valid until the screen turns off.
- **Lock after 30 seconds** - you can exit and access again your unlocked apps within 30 seconds.

If you would like to change the selected setting:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.
3. Tap **Require unlock every time** in the App Lock area.
4. Choose the desired option.

### 3.7.3. App Lock Settings

For an advanced configuration of App Lock:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.

In the App Lock area, you can configure the following options:



- **Sensitive app suggestion** - receive a lock notification each time you are installing a sensitive app.
- **Require unlock every time** - choose one of the available lock and unlock options.
- **Smart Unlock** - keep apps unlocked while you are connected to trusted Wi-Fi networks.
- **Random keyboard** - prevent PIN reading by randomizing number positions.

### 3.7.4. Snap Photo

With Bitdefender Snap Photo you can catch your friends or relatives on the hop. This way you can educate their curious eyes to not look through your personal files or the apps you use.



The feature works easy: each time the PIN code or fingerprint confirmation you set to protect your apps is entered wrong three times in a row, a photo is taken using the front camera. The photo is saved together with the time-stamp and reason, and can be seen when you open Bitdefender Mobile Security and access the App Lock feature.



#### Note

This feature is available only for phones that have a front camera.

To configure the Snap Photo feature for App Lock:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.
3. Enable the corresponding switch in the Snap Photo area.

The photos snapped when the incorrect PIN is entered are displayed in the App Lock window and can be viewed full-screen.

Alternatively, they can be viewed in your Bitdefender account:



1. Go to: <https://central.bitdefender.com>.
2. Sign in to your account.
3. Select the **My Device** panel.
4. Select your Android device, and then the **Anti-Theft** tab.



5. Tap  next to **Check your snapshots** to view the latest photos that were taken.

Only the two most recent photos are saved.

To stop uploading snapped photos on your Bitdefender account:




1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.
3. Disable **Upload photos** in the Snap Photo area.

### 3.7.5. Smart Unlock

An easy method to stop being asked by the App Lock feature to enter the PIN code or fingerprint confirmation for the protected apps each time you access them is to activate Smart Unlock.

With Smart Unlock you can set as trusted the Wi-Fi networks you usually connect to, and when connected to them, the App Lock blocking settings will be disabled for the protected apps.

To configure the Smart Unlock feature:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **App Lock**.
3. Tap the  button.
4. Tap the switch next to **Smart Unlock**, if the feature is not yet enabled. Validate using your fingerprint or your PIN.  
The first time you'll activate the feature, you will need to enable the location permission. Tap the **ALLOW** button, then tap **ALLOW** again.
5. Tap **ADD** to set the Wi-Fi connection you're currently using as trusted.

Whenever you change your mind, disable the feature and the Wi-Fi networks you have set as trusted will be treated as untrusted.



## 3.8. Reports

The Reports feature keeps a detailed log of events concerning the scanning activity on your device.

Whenever something relevant to the security of your device happens, a new message is added to the Reports.



To access the Reports section:



1. Tap  **More** on the bottom navigation bar.
2. Tap  **Reports**.

The following tabs are available in the Reports window:

- **WEEKLY REPORTS** - here you have access to the security status and the performed tasks from the current and previous week. The current week's report is generated each Sunday and you will receive a notification informing you about it becoming available.



Each week a new tip will be displayed in this section, so make sure you check back regularly to get the best out of the app.

To stop receiving notifications each time a report is generated:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.
3. Disable the **New report notification** switch in the Reports area.

- **ACTIVITY LOG** - here you can check detailed information about the activity of your Bitdefender Mobile Security app since it was installed on your Android device.

To delete the available activity log:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.
3. Tap **Clear Activity Log**, and then tap **CLEAR**.

### 3.9. WearON

With Bitdefender WearON you can easily find your smartphone whether you left it at the office in a conference room or under a pillow on your couch. The device can be found even if the silent mode is activated.

Keep this feature enabled to make sure that you always have your smartphone at hand.



#### Note

The feature works with Android 4.3 and Android Wear.



### 3.9.1. Activating WearON

To use WearON, you only have to connect your smartwatch to the Bitdefender Mobile Security app and activate the feature with the following voice command:

Start:<Where is my phone>

**Bitdefender WearON** has two commands:

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

With the Phone Alert feature you can quickly find your smartphone whenever you step too far away from it.

If you have your smartwatch with you, it automatically detects the app on your phone and vibrates whenever you go too far from your phone, more exactly when the Bluetooth connectivity is lost.



To enable this feature, open Bitdefender Mobile Security, tap **Global Settings** in the menu and select the corresponding switch under the WearON section.

#### 2. **Scream**

Finding your phone has never been easier. Whenever you forget where you left your phone, tap the Scream command on your watch to make your phone scream.

### 3.10. About

To find information about the Bitdefender Mobile Security version you have installed, to access and read the Subscription Agreement and Privacy Policy, and view the Open-source licenses:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.
3. Tap the desired option in the About area.



## 4. FREQUENTLY ASKED QUESTIONS

### **Why does Bitdefender Mobile Security require an internet connection?**



The app needs to communicate with Bitdefender servers to determine the security status of the apps it scans and of the webpages you are visiting, and also to receive commands from your Bitdefender account, when using the Anti-Theft features.

### **What does Bitdefender Mobile Security need each permission for?**

- Internet access -> used for cloud communication.
- Read phone state and identity -> used to detect if the device is connected to the internet and to extract certain device info needed to create a unique ID when communicating to Bitdefender cloud.
- Read and write browser bookmarks -> Web Protection module deletes malicious sites from your browsing history.
- Read log data -> Bitdefender Mobile Security detects traces of threat activities from the Android logs.
- Location -> required for remote location.
- Camera -> required for Snap photo.
- Storage -> used to allow the Malware Scanner to check the SD card.

### **How can I stop submitting to Bitdefender information about suspect apps?**



By default, Bitdefender Mobile Security sends reports to Bitdefender servers about the suspect apps you are installing. This information is essential for improving the threat detection and can help us to offer you a better experience in the future. In case you want to stop sending us information about suspect apps:

1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.
3. Turn off **In-the-cloud detection** in the Malware Scanner area.


### **Where can I see details about the app's activity?**

Bitdefender Mobile Security keeps a log of all important actions, status changes, and other critical messages related to its activity. To access see about the app's activity:





1. Tap  **More** on the bottom navigation bar.
2. Tap  **Reports**.  
In the WEEKLY REPORTS window you can access the reports that are generated every week and in the ACTIVITY LOG window you can view information about the activity of your Bitdefender app.

### **I forgot the PIN code that I set to protect my app. What do I do?**

1. Access [Bitdefender Central](#).
2. Select the **My Devices** panel.
3. Tap the desired device card, and then tap  in the upper-right corner of the screen.
4. Select **Settings**.
5. Retrieve the PIN code from the **Application PIN** field.

### **How can I change the PIN code I set for App Lock and Anti-Theft?**

If you wish to change the PIN code you set for App Lock and Anti-Theft:




1. Tap  **More** on the bottom navigation bar.
2. Tap  **Settings**.
3. Tap Security **PIN CODE** in the Anti-Theft area.
4. Type in the current PIN code.
5. Type in the new PIN code you want to set.

### **How can I switch off the App Lock feature?**

There is no turn off option for the App Lock feature, but you can easily disable it by clearing the check boxes next to the selected apps after validating the PIN or fingerprint you have set.

### **How can I set another wireless network as trusted?**

First, you have to connect your device to the wireless network you want to set as trusted. Then follow these steps:


1. Tap  **More** on the bottom navigation bar.
2. Tap  **App Lock**.
3. Tap  in the upper-right corner.



4. Tap **ADD** next to the network you want to set as trusted.

### **How can I stop seeing snapped photos taken on my devices?**

To stop making visible the snapped photos taken on your devices:

1. Access [Bitdefender Central](#).
2. Tap  in the upper right side of the screen.
3. Tap **Settings** in the slide menu.
4. Disable the **Show/don't show snap photos taken on your devices** option.

### **How can I keep my online shopping secure?**

Online shopping comes with high risks when some details are ignored. To not become a victim of fraud, we recommend you the following:

- Keep your security app updated.
- Submit online payments only with buyer protection.
- Use a VPN when connecting to the internet from public and unsecured wireless networks.
- Pay attention to the passwords you have assigned to your online accounts. They have to be strong including capital and lowercase letters, numbers and symbols (@, !, %, #, etc.).
- Make sure that the information you send is over secure connections. The online website extension has to be HTTPS://, and not HTTP://.

### **When should I use Bitdefender VPN?**

You have to be careful when you access, download, or upload content on the internet. To make sure you stay safe while browsing the web, we recommend you to use Bitdefender VPN when you:

- want to connect to public wireless networks
- want to access content that normally is restricted in specific areas, no matter you are home or abroad
- want keep your personal data private (usernames, passwords, credit card information, etc.)
- want to hide your IP address

### **Will Bitdefender VPN have a negative impact on the battery life of my device?**




Bitdefender VPN is designed to protect your personal data, hide your IP address while connected to unsecured wireless networks, and access restricted content in certain countries. To avoid an unnecessary battery consumption of your device, we recommend you to use the VPN only when you need it, and disconnect when offline.

### **Why am I encountering internet slowdowns while connected with Bitdefender VPN?**

Bitdefender VPN is designed to offer you a light experience while surfing the web; however, your internet connectivity or the server distance you connect to may cause the slowdown. In this case, if it is not a must to connect from your location to a faraway hosted server (e.g. from USA to China), we recommend you to allow Bitdefender VPN to automatically connect you to the nearest server, or find a server closer to your current location.

### **Can I change the Bitdefender account linked to my device?**

Yes, you can easily change the Bitdefender account linked to your device by following these steps:

1. Tap  **More** on the bottom navigation bar.
2. Tap your email address.
3. Tap **Log out of your account**. If a PIN code has been set, you are prompted to type it.
4. Confirm your choice.
5. Type the email address and the password of your account in the corresponding fields, and then tap **SIGN IN**.

### **How will Bitdefender Mobile Security impact my device's performance and battery autonomy?**

We keep the impact very low. The app only runs when it is essential - after you install an app, when you browse the app interface or when you want a security check. Bitdefender Mobile Security does not run in the background when you call your buddies, type a message or play a game.

### **What is Device Administrator?**

Device Administrator is an Android feature that gives Bitdefender Mobile Security the permissions needed to perform certain tasks remotely. Without these privileges, remote lock would not work and device wipe



would not be able to completely remove your data. If you want to remove the app, make sure to revoke these privileges before trying to uninstall from **Settings > Security > Select device administrators**.

### **How to fix "No Google Token" error that appears when signing in to Bitdefender Mobile Security.**

This error occurs when the device is not associated with a Google account, or the device is associated with an account but a temporary problem is preventing it from connecting to Google. Try one of the following solutions:

- Go to Android Settings > Applications > Manage Applications > Bitdefender Mobile Security and tap **Clear data**. Then try to sign in again.
- Make sure your device is associated with a Google account.  
To check this, go to Settings > Accounts & sync and see if a Google account is listed under **Manage Accounts**. Add your account if one is not listed, restart your device and then try to sign in to Bitdefender Mobile Security.
- Restart your device, and then try to sign in again.

### **In what languages is Bitdefender Mobile Security available?**

Bitdefender Mobile Security is currently available in the following languages:

- Brazilian
- Czech
- Dutch
- English
- French
- German
- Greek
- Hungarian
- Italian
- Japanese
- Korean
- Polish



- ☐ Portuguese
- ☐ Romanian
- ☐ Russian
- ☐ Spanish
- ☐ Swedish
- ☐ Thai
- ☐ Turkish
- ☐ Vietnamese

Other languages will be added in future releases. To change the language of the Bitdefender Mobile Security interface, go to your device's **Language & keyboard** settings and set the device to the language you want to use.



## 5. GETTING HELP

### 5.1. Asking for Help

Bitdefender provides its customers with an unparalleled level of fast and accurate support. If you experience any issue or if you have any question about your Bitdefender product, you can use several online resources to find a solution or an answer.

### 5.2. Online Resources

Several online resources are available to help you solve your Bitdefender-related problems and questions.

- Bitdefender Support Center:  
<https://www.bitdefender.com/consumer/support/>
- The Bitdefender Expert Community:  
<https://community.bitdefender.com/en/>
- Bitdefender Cyberpedia:  
<https://www.bitdefender.com/cyberpedia/>

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

#### 5.2.1. Bitdefender Support Center

The Bitdefender Support Center is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the Bitdefender support and development teams, along with more general articles about threat prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Support Center is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Support Center, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.



The Bitdefender Support Center is available any time at at the following address: <https://www.bitdefender.com/consumer/support/>.

### 5.2.2. The Bitdefender Expert Community

The Expert Community is an environment where Bitdefender users, enthusiasts and fans can engage, exchange ideas, support each other and share their knowledge and solutions. It is also a place of ideation and provides valuable feedback to our development teams. The community members are experienced Bitdefender users happy to help other peers on their own time.

Here you will find meaningful conversations with people that use Bitdefender on their devices. The community offers a true connection with our members and makes your voice heard. It is a place where you are encouraged to participate knowing that your opinion and input are respected and cherished. As a valued provider, we strive to offer an unparalleled level of fast, accurate support and we wish to bring our users closer to us. We have designed our community with this purpose in mind.

You can find our Expert Community webpage here:

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

### 5.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia has all the info you need about the latest cyber-threats. This is the place where Bitdefender experts share tips & tricks about how to stay protected from hackers, data breaches, identity theft and social impersonation attempts.

The Bitdefender Cyberpedia webpage can be found here:

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

## 5.3. Contact Information

Efficient communication is the key to a successful business. Since 2001 BITDEFENDER has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us directly through our **Bitdefender Support Center**:

<https://www.bitdefender.com/consumer/support/>



### 5.3.1. Local distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to <https://www.bitdefender.com/partners/partner-locator.html>.
2. Choose your country and city using the corresponding options.



## GLOSSARY

### **Activation code**

Is a unique key that can be bought from retail and used to activate a specific product or service. An activation code enables the activation of a valid subscription for a certain period of time and number devices and can also be used to extend a subscription with the condition to be generated for the same product or service.

### **ActiveX**

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive webpages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the webpage. ActiveX controls are often written using Visual Basic. Active X is notable for a complete lack of security controls; computer security experts discourage its use over the internet.

### **Advanced persistent threat**

Advanced persistent threat (APT) exploits vulnerabilities of systems to steal important information to deliver it to the source. Big groups such as organizations, companies, or governments, are targeted by this threat. The objective of an advanced persistent threat is to remain undetected for a long time being able to monitor and gather important information without damaging the targeted machines. The method used to inject the threat into the network is through a PDF file or an Office document that look harmless so that every user can run the files.

### **Adware**

Adware is often combined with a host app that is provided at no charge as long as the user agrees to accept the adware. Because adware apps are usually installed after the user has agreed to a licensing agreement that states the purpose of the app, no offense is committed. However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these apps collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.



## **Archive**

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

## **Backdoor**

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

## **Boot sector**

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

## **Boot virus**

A threat that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the threat to become active in memory. Every time you boot your system from that point on, you will have the threat active in memory.

## **Botnet**

The term “botnet” is composed of the words “robot” and “network”. Botnets are internet-connected devices infected with threats and can be used to send spam emails, steal data, remotely control vulnerable devices, or spread spyware, ransomware, and other kinds of threats. Their objective is to infect as many connected devices as possible, such as PCs, servers, mobile or IoT devices belonging to big companies or industries.

## **Browser**

Short for web browser, a software app used to locate and display webpages. Popular browsers include Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. These are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.



### **Brute Force Attack**

Password guessing attack used to break into a computer system by entering possible password combinations, mostly starting with the easiest-to-guess password.

### **Command line**

In a command line interface, the user types commands in the space provided directly on the screen using command language.

### **Cookies**

Within the internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

### **Cyberbullying**

When peers or strangers are committing abusive acts against children on purpose to physically hurt them. To damage emotionally, the assaulters are sending mean messages or unflattering photos, thus making their victims isolate from others or feel frustrated.

### **Dictionary Attack**

Password guessing attacks used to break into a computer system by entering a combination of common words to generate potential passwords. The same method is used to guess decryption keys of encrypted messages or documents. Dictionary attacks succeed because many people incline to choose short and single words passwords that are easy to be guessed.

### **Disk drive**

It's a machine that reads data from and writes data onto a disk. A hard disk drive reads and writes hard disks. A floppy drive accesses floppy



disks. Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

### **Download**

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

### **Email**

Electronic mail. A service that sends messages on computers via local or global networks.

### **Events**

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

### **Exploits**

A way to take advantage of different bugs or vulnerabilities that are present in a computer (software or hardware). Thus, hackers may gain the control of computers or networks.

### **False positive**

Occurs when a scanner identifies a file as infected when in fact it is not.

### **Filename extension**

The portion of a filename, following the final point, which indicates the kind of data stored in the file. Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

### **Heuristic**

A rule-based method of identifying new threats. This method of scanning does not rely on specific threat information database. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing threat. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".



## **Honeypot**

A decoy computer system set to attract hackers to study the way they act and identify the heretical methods they use to collect system information. Companies and corporations are more interested in implementing and using honeypots to improve their overall state of security.

## **IP**

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

## **Java applet**

A Java program which is designed to run only on a webpage. To use an applet on a webpage, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the webpage is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from apps in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

## **Keylogger**

A keylogger is an app that logs anything you type. Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

## **Macro virus**

A type of computer threat that is encoded as a macro embedded in a document. Many apps, such as Microsoft Word and Excel, support powerful macro languages. These apps allow you to embed a macro in a document, and have the macro execute each time the document is opened.

## **Mail client**

An email client is an app that enables you to send and receive email.



### **Memory**

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

### **Non-heuristic**

This method of scanning relies on specific threat information database. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a threat, and does not generate false alarms.

### **Online predators**

Individuals who seek to attract minors or adolescents into conversations on purpose to involve them into illegal sexual activities. Social networks are the ideal place where vulnerable children can easily be hunted and seduced into committing sexual activities, online or face-to-face.

### **Packed programs**

A file in a compression format. Many operating systems and apps contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

### **Path**

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

### **Phishing**

The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security, and



bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the user's information.

### **Photon**

Photon is an innovative non-intrusive Bitdefender technology, designed to minimize the performance impact of your security solution. By monitoring your PC's activity in the background, it creates usage patterns that help optimize booting and scanning processes.

### **Polymorphic virus**

A threat that changes its form with each file it infects. Since they have no consistent binary pattern, such threats are hard to identify.

### **Port**

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

### **Ransomware**

Ransomware is a malicious program that tries to make money from users by locking their vulnerable systems. CryptoLocker, CryptoWall, and TeslaWall, are only some variants that hunt personal systems of users.

The infection can be spread by accessing spam emails, downloading email attachments, or installing apps, without letting the user know about what is happening on his system. Daily users and companies are targeted by ransomware hackers.

### **Report file**

A file that lists actions that have occurred. Bitdefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

### **Rootkit**

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and



it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some apps hide critical files using rootkits. However, they are mostly used to hide threats or to conceal the presence of an intruder into the system. When combined with threats, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

### **Script**

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

### **Spam**

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited email.

### **Spyware**

Any software that covertly gathers user information through the user's internet connection without his or her knowledge, usually for advertising purposes. Spyware apps are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet; however, it should be noted that the majority of shareware and freeware apps do not come with spyware. Once installed, the spyware monitors user activity on the internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse threat is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's internet connection. Because spyware is using memory and



system resources, the apps running in the background can lead to system crashes or general system instability.

### **Startup items**

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or apps can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

### **Subscription**

Purchase agreement that gives the user the right to use a particular product or service on a specific number of devices and for a certain period of time. An expired subscription can be automatically renewed using the information provided by the user at the first purchase.

### **System tray**

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

### **TCP/IP**

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

### **Threat**

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most threats can also replicate themselves. All computer threats are manmade. A simple threat that can copy itself over and over again is relatively easy to produce. Even such a simple threat is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of threat is one capable of transmitting itself across networks and bypassing security systems.



### **Threat Information Update**

The binary pattern of a threat, used by the security solution to detect and eliminate the threat.

### **Trojan**

A destructive program that masquerades as a benign app. Unlike malicious software programs and worms, Trojans do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse threats is a program that claims to rid your computer of threats but instead introduces threats onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

### **Update**

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has its own update feature that allows you to manually check for updates, or let it automatically update the product.

### **Virtual Private Network (VPN)**

Is a technology that enables a temporary and encrypted direct connection to a certain network over a less secure network. This way, sending and receiving data is secure and encrypted, difficult to be caught by snoopers. A proof of security is the authentication, which can be done only using a username and password.

### **Worm**

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.