

USER'S GUIDE

**Bitdefender**® CONSUMER  
SOLUTIONS

# Mobile Security for iOS





# Bitdefender Mobile Security for iOS

## 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**<sup>®</sup>



# 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 for iOS ..... 3**
- 2. Getting Started ..... 4**
  - 2.1. Device Requirements ..... 4
  - 2.2. Installing Bitdefender Mobile Security for iOS ..... 4
  - 2.3. Sign in to your Bitdefender account ..... 5
  - 2.4. Dashboard ..... 6
- 3. Features & Functionalities ..... 8**
  - 3.1. Scan ..... 8
  - 3.2. Scam Alert ..... 8
    - 3.2.1. How to set up Scam Alert ..... 9
  - 3.3. Web Protection ..... 10
    - 3.3.1. Bitdefender alerts ..... 11
  - 3.4. VPN ..... 12
    - 3.4.1. Subscriptions ..... 14
  - 3.5. Account Privacy ..... 15
- 4. Frequently Asked Questions ..... 17**
- 5. Getting Help ..... 18**
  - 5.1. Asking for Help ..... 18
  - 5.2. Online Resources ..... 18
    - 5.2.1. Bitdefender Support Center ..... 18
    - 5.2.2. The Bitdefender Expert Community ..... 19
    - 5.2.3. Bitdefender Cyberpedia ..... 19
  - 5.3. Contact Information ..... 19
    - 5.3.1. Local distributors ..... 20
- Glossary ..... 21**



## ABOUT THIS GUIDE

### Purpose and Intended Audience

This guide is intended to all iOS users who have chosen Bitdefender Mobile Security for iOS 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 Apple mobile devices.

You will find out how to configure and use Bitdefender Mobile Security for iOS 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 for iOS and its user interface.

[Features & Functionalities \(page 8\)](#)

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

[Getting Help \(page 18\)](#)

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 FOR IOS

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 for iOS allows you to:

- Gain the most powerful protection against threats with the least impact on battery
- Protect your personal data: passwords, address, social and financial information
- Easily check your phone security to detect and fix misconfigurations that might expose it
- Avoid accidental data exposure and misuse for all installed apps
- Scan your device to achieve optimal security and privacy settings
- Gain usage insights into your online activity and history of prevented incidents
- Check your online accounts against data breaches or data leaks
- Encrypt internet traffic with the included VPN

Bitdefender Mobile Security for iOS is delivered free of charge and requires activation with a [Bitdefender account](#). However, some important features of Bitdefender, such as our 'Web Protection' module, require a paid subscription in order to be accessible to our users.



## 2. GETTING STARTED

### 2.1. Device Requirements

Bitdefender Mobile Security for iOS works on any device running iOS 12 or later versions of the operating system and needs an active internet connection to be activated and to detect if any data leakage has occurred in your online accounts.

### 2.2. Installing Bitdefender Mobile Security for iOS

#### ○ From Bitdefender Central

##### ○ On iOS

1. Access [Bitdefender Central](#).
2. Select the **My Devices** panel.
3. Tap **INSTALL PROTECTION**, and then tap **Protect this device**.
4. Select the owner of the device. If the device belongs to someone else, tap the corresponding button.
5. You are redirected to the **App Store** app. In the App Store screen, tap the installation option.

##### ○ On Windows, macOS, Android

1. Access [Bitdefender Central](#).
2. Select the **My Devices** panel.
3. Press **INSTALL PROTECTION**, and then press **Protect other devices**.
4. Select the owner of the device. If the device belongs to someone else, press the corresponding button.
5. Press **SEND DOWNLOAD LINK**.
6. 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.



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

## ○ From App Store

Search for Bitdefender Mobile Security for iOS to locate and install the app.

An introduction window containing details about the product features is displayed the first time you open the app. Tap Get started to proceed to the next window.

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 for iOS.

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

## 2.3. Sign in to your Bitdefender account

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

To link your device to a Bitdefender account:

1. Type your Bitdefender account email address in the corresponding field, and then tap **NEXT**. If you do not have a Bitdefender account and want to create one, select the corresponding link, and then follow the onscreen instructions until the account is activated.

To sign in using a Facebook, Google, Apple, or Microsoft account, tap the service you want to use from the **Or sign in with** area. You are redirected to the sign in page of the selected service. Follow the instructions to link your account to Bitdefender Mobile Security for iOS.



### 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. Type your password, and then tap **SIGN IN**.

From here you can also access the Bitdefender Privacy Policy.

## 2.4. Dashboard

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

The first time you access the app, you are prompted to allow Bitdefender to send you notifications. Tap **Allow** to stay informed each time Bitdefender has to communicate you something relevant to your app. To manage Bitdefender notifications, go to Settings > Notifications > Mobile Security.

To get access to the section you need, tap the corresponding icon from the bottom of the screen.

### Web Protection

Stay safe while you surf the web and whenever less secure apps will try to access untrusted domains. For more information, refer to [Web Protection \(page 10\)](#).

### VPN

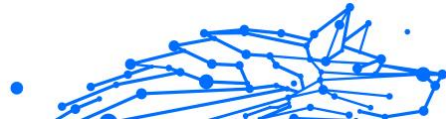
Maintain your privacy no matter what network you are connected to by keeping your internet communication encrypted. For more information, refer to [VPN \(page 12\)](#).

### Account Privacy

Find out whether your email accounts have been leaked or not. For more information, refer to [Account Privacy \(page 15\)](#).

To see additional options, tap the **☰** icon on your device while in the application's home screen. The following options appear:

- **Restore purchases** - from here you can restore the previous subscriptions you have purchased through your iTunes account.
- **Settings** - from here you have access to:
  - **VPN Settings**
    - **Agreement** - you can read the terms under which you use the Bitdefender VPN service. If you tap **I don't agree anymore**, you



will not be able to use Bitdefender VPN at least until you tap **I Agree**.

- **Open Wi-Fi warning** - you can enable or disable the product notification that appears each time you connect to an unsecured Wi-Fi network.

The purpose of this notification is to help you keep your data private and secure by using Bitdefender VPN.

- **Web Protection Settings**

- **Agreement** - you can read the terms under which you use the Bitdefender Web Protection service. If you tap **I don't agree anymore**, you will not be able to use Bitdefender VPN at least until you tap **I Agree**.

- **Enable Web Protection notification** - Notifies you that Web Protection can be enabled after finishing a VPN session.

- **Product reports**

- **Feedback** - from here you can launch the default email client to send us your feedback about the app.
- **App info** - from here, you have access to information about the installed version and to Subscription Agreement, Privacy Policy, and Open-source licenses compliances.



## 3. FEATURES & FUNCTIONALITIES

### 3.1. Scan

Bitdefender Mobile Security for iOS allows you to scan your device for any security vulnerabilities and potential threats on your device. Running the scan will check for:

- **OS version:** Checking your iOS version for the latest updates.
- **Passcode/Biometrics:** Checking the security level in regards to accessing your device.
- **Web Protection:** Checking the state of the Web Protection module
- **Account Privacy:** Checking for the presence of monitored accounts listed in the Account Privacy module.
- **Scan Wi-Fi:** Checking for the security status of the currently connected network.

The protection status is determined after you run a manual scan.

After running the first scan, you will be met with Bitdefender's [Autopilot recommendations](#). This is your personal security advisor, providing contextual recommendations based on your device usage and needs. This way, you'll get to benefit from everything your app has to offer.



#### Note

When first entering the app, you will be prompted to run a scan.

### 3.2. Scam Alert

The Scam Alert feature available in Bitdefender Mobile Security for iOS proactively protects Apple users from phishing scams. Scam Alert for iOS includes two layers of protection that monitor scams delivered through SMS/MMS messages and calendar invites:

- **Text Message Filter (SMS, MMS)**

This feature identifies and filters unwanted SMS and MMS messages.

A malicious SMS/MMS (Short Message Service/Multimedia Messaging Service) refers to a type of message sent to mobile devices with harmful intent. These messages are designed to exploit vulnerabilities,



deceive recipients, or cause harm to the target's device, personal information, or security.

### ○ **Calendar Invite Link Scanner**

This feature detects spam calendars and events that contain dangerous links. The calendar virus is a type of spam that affects the Calendar app of your iPhone, which can be annoying and potentially dangerous:

- You get unwanted calendar invitations or event notifications when you accidentally accept a fake calendar invite sent to your email address by hackers or spammers.
- When you click on the link in the invite, you unknowingly subscribe to the sender's calendar, which allows them to send you more spam events.
- The spam events may contain links or attachments that could lead you to phishing pages or other cyber-threats if you open them.

## 3.2.1. How to set up Scam Alert

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

### **How to enable SMS Filtering:**

In order for Bitdefender to start filtering messages, you must manually activate the Filter Unknown Senders option in Messages app settings:

1. Open the **Settings** app on your iPhone or iPad.
2. Scroll down and select **Messages** in the list.
3. Tap the **Unknown & Spam** section.
4. Toggle **Filter Unknown Senders** to the on position.
5. Select **Mobile Security** in the SMS Filtering section and then choose **Enable**.

Bitdefender will now be able to filter junk messages on your iPhone/iPad.



### **Note**

Due to iOS restrictions, Bitdefender SMS filtering can only be used for SMS and MMS messages that come from people you don't have saved in your contacts. This means it won't filter messages from people already in your contacts list or iMessage messages from anyone.



## How to enable Calendar Scan:

1. Open the **Bitdefender Mobile Security** app installed on your iPhone or iPad.
2. Go to the **Scam Alert** option in the bottom navigation bar and press **Set up now**.
3. Tap **Continue**, and then tap **Enable**.
4. Choose **OK** to grant Bitdefender access to your calendar. A calendar scan will begin immediately.

## 3.3. Web Protection

Bitdefender Web Protection ensures a safe browsing experience by alerting you about potential malicious webpages and when less secure installed apps will try to access untrusted domains.


When an URL points to a known phishing or fraudulent website, or to malicious content such as spyware or viruses, the webpage is blocked and an alert is shown. The same thing happens when installed apps try to access malicious domains.



### Important

If you are located in an area where the usage of a VPN service is restricted by law, the functionality of Web Protection will not be available.

To activate Web Protection:

1. Tap the  icon from the bottom of the screen.
2. Tap **I Agree**.
3. Enable the Web Protection switch.



### Note

The first time you turn on Web Protection, you might be prompted to allow Bitdefender to set up VPN configurations that will monitor network traffic. Tap **Allow**, to continue. If an authentication method (fingerprint or PIN code) has been set to protect your smartphone, you are required to use it. To be able to detect access to untrusted domains, Web Protection is working together with the VPN services.



## Important

The Web Protection feature and the VPN cannot function at the same time. Whenever one of them is enabled, the other (if it is active at that time) will be disabled.

### 3.3.1. Bitdefender alerts

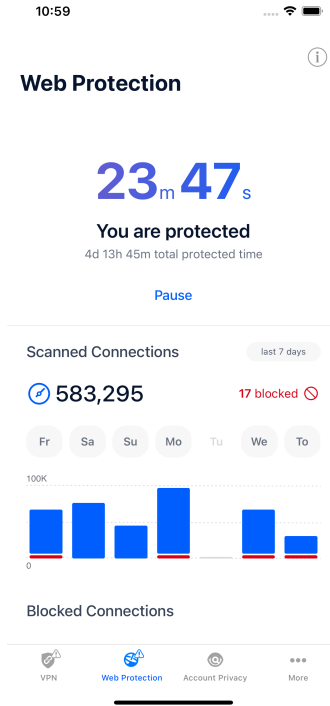
Whenever you try to visit a website classified as unsafe, the website is blocked. To make you aware of the event, you are notified by Bitdefender in the Notification center and in your browser. The warning page contains information such as the website URL and the detected threat. You have to decide what to do next.

Also, you are notified in the Notification Center whenever a less secure app tries to access untrusted domains. Tap the displayed notification to be redirected to the window where you can decide what to do next.

The following options are available for both cases:

- Navigate away from the website by tapping **TAKE ME BACK TO SAFETY**.
- Proceed to the website, despite the warning, by tapping the displayed notification, and then **I want to access the page**.

Confirm your choice.



## 3.4. 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 military-grade encryption, and hiding your IP address wherever you are. Your traffic is redirected through a separate server; thus making your device impossible to be identified by your ISP, through the myriad of other devices that are using our services. Moreover, while connected to the internet via Bitdefender Mobile Security for iOS, 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.


To turn on Bitdefender VPN:

1. Tap the  icon from the bottom of the screen.
2. 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

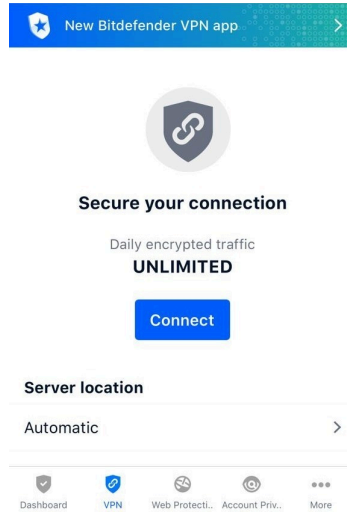
The first time you turn on VPN, you are prompted to allow Bitdefender to set up VPN configurations that will monitor network traffic. Tap **Allow**, to continue. If an authentication method (fingerprint or PIN code) has been set to protect your smartphone, you are required to use it.

The  icon appears in the status bar when VPN is active.

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

If you have a premium subscription and would like to connect to a server at your will, tap Automatic in the VPN interface, and then select the location you want. For details about VPN subscriptions, refer to [Subscriptions \(page 14\)](#).





## 3.4.1. 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 the **Activate Premium VPN** button available in the VPN window. There are two types of subscriptions to choose from: annual and monthly.

The Bitdefender Premium VPN subscription is independent from the Bitdefender Mobile Security for iOS free subscription, meaning you will be able to use it for its entire availability. In case the Bitdefender Premium VPN subscription expires, your will be automatically 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.


## 3.5. Account Privacy

Bitdefender Account Privacy detects if any data leakage 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.

To check if any of accounts has been leaked, tap **Scan for leaks**.

To start keeping personal information safe:

1. Tap the  icon from the bottom of the screen.
2. Tap **Add account**.
3. Type your email address in the corresponding field, and then tap **Next**. Bitdefender needs to validate this account before displaying private information. Therefore, an email with a validation code is sent to the provided email address.
4. 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 too.


The privacy status of the validated account is displayed.

If leaks 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 leak(s) as **Solved**. To do this:



1. Tap  next to the breach you solved.
2. Tap **Mark as solved**.

When all the detected leaks are marked as Solved, the account will no longer appear as leaked, at least until a new leakage is detected.



## 4. FREQUENTLY ASKED QUESTIONS

### **How does Bitdefender Mobile Security for iOS protect me against viruses and cyber threats?**

Bitdefender Mobile Security for iOS provides absolute protection against all cyber threats and is especially designed to keep your sensitive data safe from prying eyes.

You get a wealth of advanced security and privacy features for your iPhone and iPad - plus many bonus features, including VPN and Web Protection.

Bitdefender Mobile Security for iOS reacts instantly to viruses and malware with no compromise to your system's performance.

### **What type of devices and operating systems does Bitdefender Mobile Security for iOS cover?**

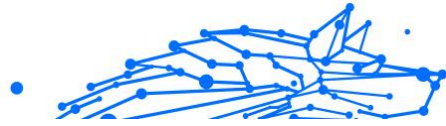
Bitdefender Mobile Security for iOS will protect your smartphones and tablets running iOS against all cyber threats.

### **Why do I need Bitdefender Mobile Security for iOS on Apple OS?**

Some of your most personal data is stored on your iPhone or iPad - and you need to know it is safe at all times. Bitdefender Mobile Security for iOS provides absolute protection against cyber threats and takes care of your online privacy and private information without interfering in your day-to-day activities.

### **Do I get a VPN with my Bitdefender Mobile Security for iOS subscription?**

Bitdefender Mobile Security for iOS comes with a basic version of Bitdefender VPN that includes a generous amount of traffic (200 MB/ day, a total of 6GB/ month) free of charge.



## 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**

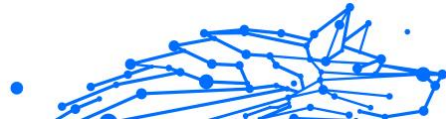
A threat that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the threat to become active in memory. Every time you boot your system from that point on, you will have the threat active in memory.

### **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**

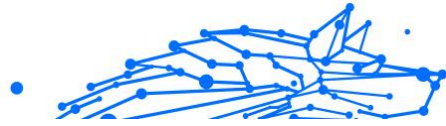
A keylogger is an app that logs anything you type. Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private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