USER'S GUIDE

Bitdefender CONSUMER SOLUTIONS

Identity Theft Protection

Bitdefender Identity Theft Protection

User's Guide

Publication date 09/06/2023

Legal Notice

Bitdefender

Table of Contents

ABOUT THIS GUIDE

Purpose and Intended Audience

This guide is intended to all Bitdefender users who have chosen Bitdefender Identity Theft Protection as their dedicated tool for keeping them safe against the rising tide of online data breaches and online theft. The information presented in this book is suitable not only for computer literate, but rather it is accessible to everyone.

This guide is specifically designed to help you navigate, use, and get the overall best out of Bitdefender Identity Theft Protection.

Wewish you a pleasand and useful lecture.

How to Use This Guide

This guide is organized around several major topics:

Getting Started (page 5)

Get started with setting up your Bitdefender Identity Theft Protection.

Navigate & Use (page 10)

Learn how to use and navigate Bitdefender Identity Theft Protection in order to keep your identity and personal data safe at all times.

Getting Help (page 19)

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.
https://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
documentation@bitdefender.com	Email addresses are inserted in the text for contact information.
About this Guide (page 1)	This is an internal link, towards some location inside the document.
filename	File and directories are printed using monospaced font.
option	All the product options are printed using **bold** characters.
keyword	Important keywords or phrases are highlighted using **bold** 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. Write all of your documentation-related emails in English so that we can process them efficiently.

1. WHAT IS BITDEFENDER IDENTITY THEFT PROTECTION

Bitdefender Identity Theft Protection is our security solution designed to protect you against the considerable rise of identity theft incidents.

Bitdefender Identity Theft Protection powered by IdentityForce delivers ongoing monitoring, rapid alerts, and recovery services to help protect against Identity theft. You can rest easy knowing we are top-rated and have proven identity, privacy, and credit security solutions. We combined advanced detection technology, real-time alerts, 24/7 U.S.-based Certified Protection Experts, and identity recovery with decades of experience to get the job done.

We operate a risk-based information systems security management program that implements industry-standard best practices for protecting member data.

- Administrative & technical controls include those outlined in PCI DSS v3.2 requirements and ISO 27002 security techniques.
- Sensitive PII is encrypted with the AES symmetric encryption algorithm using 256-bit sized keys.
- Custom master keys are created for all encrypted volumes and any snapshots created from them.

Bitdefender Identity Theft Protection is available for US only. Registration requires a valid Social Security Number.

> **Note**
> Bitdefender Identity Theft Protection is available on Chrome, Firefox, Microsoft Edge and Safari.

1.1. Standard and Premium Plans

The main difference between the Standard and Premium Plans is that Premium includes **$2 million** of insurance to cover expenses incurred by identity theft as well as identity theft monitoring, credit reports & scores from 3 Credit Bureaus:

- Equifax

- Experian
- TransUnion

Our Standard plan comes with **$1 million** in identity theft insurance and a single Bureau Credit report monitoring.

Other notable differences between the two Plans are found in Premium also giving you access to additional features such as:

- Bank, credit cards & investments alerts
- Change of Address Monitoring
- Court Records Monitoring
- Sex Offender Registry Monitoring
- Ransomware Resolution & Refund (up to $25,000)
- Social Engineering Resolution & Refund (up to $25,000)

2. GETTING STARTED

2.1. Activate & Set Up

Before we can begin protecting your identity, you'll need to fully and accurately complete your registration.

Here you will find the steps required in becoming a Bitdefender Identity Theft Protection member.

Step 1

First, you will receive a confirmation email sent to the e-mail address you used when you initially signed up.

Click on the **GET STARTED** button at the top of the welcome email to activate your subscription.

Step 2

This will take you to https://central.bitdefender.com.

Sign in with your Bitdefender Central account. If you don't have an account, choose to create one.

Step 3

After signing in, the subscription is automatically activated and attached to your Bitdefender Central account.

Next, you must accept the terms & conditions before you can continue. Be sure to thoroughly review before proceeding. Check the box and then click **Agree & Continue**.

Step 4

You will then be guided to set up Bitdefender Identity Theft Protection.

Get started by completing your personal information. Add your:

- name
- date of birth
- primary phone number

- social security number
- address

Click **Done** and Bitdefender Identity Theft Protection will start monitoring your information right away.

2.2. Ensure your identity is fully protected

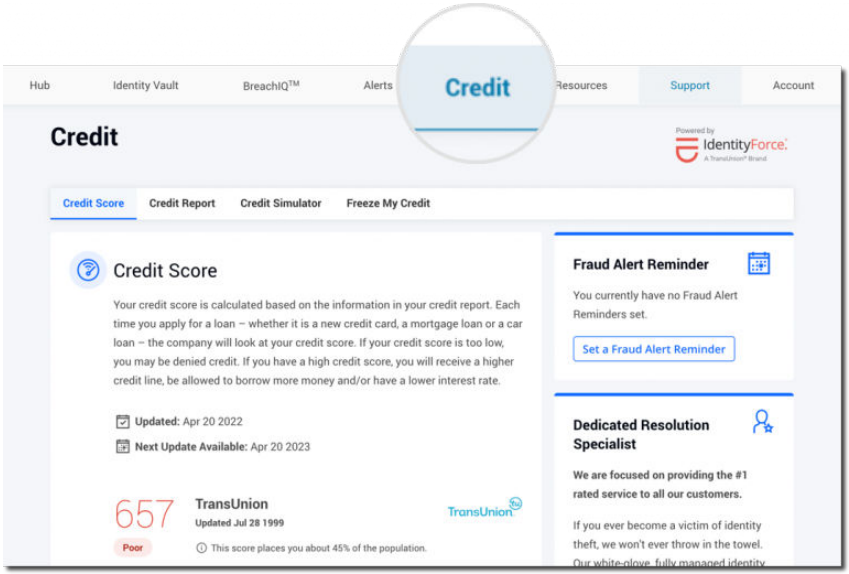
Once the setup is complete, you will be taken to your Bitdefender Central account dashboard.

Here you can further customize your protection settings, see alerts and manage your account, ensuring your identity is being fully protected by Bitdefender Identity Theft Protection.

2.2.1. Authenticate Card

First, you'll need to verify your identity to grant access to your credit reports. Here's how:

1. Start by clicking the **CREDIT** tab on the Bitdefender Identity Theft Protection dashboard. You'll now see the **Credit Score** in the reports area.



2. Next, click on **Authenticate**.
3. Read through the disclosure agreement and click **I Agree**.
4. Next, type in your Social Security number twice and click on **Activate**.
5. You'll now be asked to answer the security questions with the responses that best match your credit history.
6. Click **Submit** when you're done.

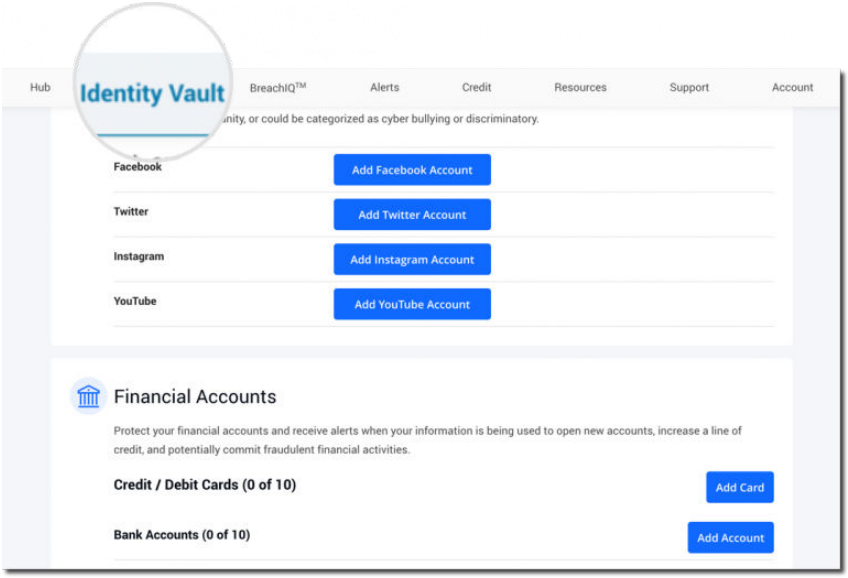
Upon successful verification, Bitdefender Identity Theft Protection will constantly monitor your credit files every day.

You will have full access to your credit scores and reports within your Bitdefender Identity Theft Protection dashboard, and you will receive alerts by email should any changes be detected.

2.2.2. Account Number Monitoring

Up next is setting up your account number monitoring. As you do this, Bitdefender Identity Theft Protection does not grant unauthorized access to any of your sensitive personal information. This functionality is critical as it detects the illegal trading and selling of your bank accounts and credit cards on the Dark Web and other data sites.

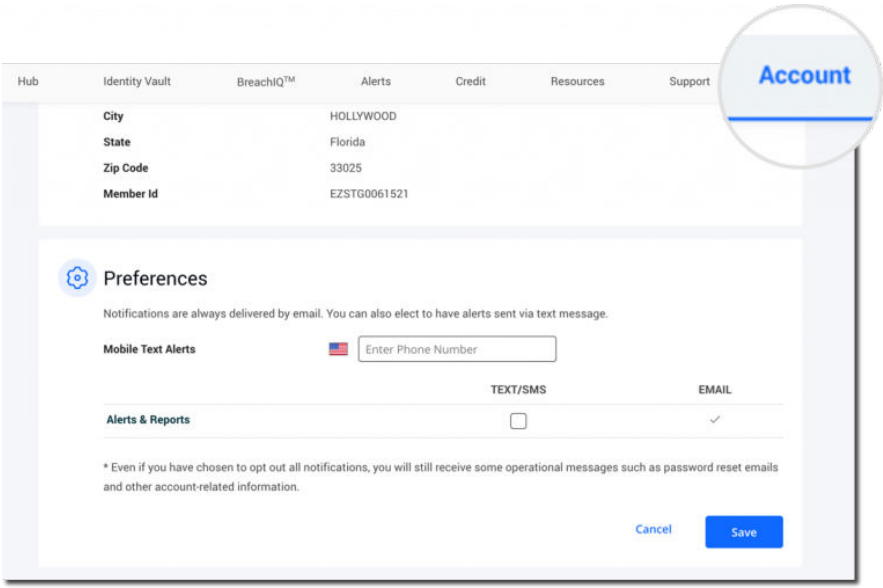
1. First, click the **IDENTITY VAULT** tab on the Bitdefender Identity Theft Protection dashboard.
2. Then scroll down to **Financial Accounts**.



3. Click **Add Card** for credit and debit cards, or **Add Account** for bank accounts.
4. Enter your card or your bank account details, then click **Save**. Once your first card/bank account has been added, you can go ahead and add more accounts or update your alert preferences.

Bitdefender Identity Theft Protection will now monitor your financial information across the Dark Web, sending you proactive alerts if any incidents are discovered.

You will receive alerts from Bitdefender based on your selected preferences. To take a look at your notification preferences, open the **ACCOUNT** tab on the Bitdefender Identity Theft Protection dashboard. Your alerts are sent to the email address shown.



Note

You can also add your mobile number for alerts via text message.

3. NAVIGATE & USE

- To check your dashboard, start by logging into your Bitdefender Central account.
  Then click Bitdefender Identity Theft Protection in the left-hand navigation column, and you'll get to your dashboard homepage.
  The **Hub** is where you will see your latest alerts and get up-to-date information on how your services are working for you.
- Quick access to a **Dedicated Resolution Specialist** can be found on the right-hand side of the Bitdefender Identity Theft Protection dashboard.
  Here you can also find **Lost Wallet Assistance**.
- To clear alerts from your dashboard, simply view the alert details and click on the Archive button.

To drill down further into your dashboard, navigate to the top menu options:

3.1. Identity Vault

In the **Identity Vault** section:

- Under **Monitored Info**, you have the option of adding personal information that you wish to continuously monitor, such as name, e-mail address, physical address, Social Security Number, credit cards, bank accounts and more.
- Under **Secure Storage**, you have the option of creating a Wallet, which can contain almost all of the aforementioned information, so that everything can be easily accessed and managed. In addition, you can also upload financial and medical records, so that they are secure and easily retrievable.

3.2. BreachIQ

Under **BreachIQ**, you will be able to find any data breach they may have been a part of and more.

Risk Rating Summary is an analysis that allows you to see the impact of the data breach on your identity's safety.

Action Plan contains detailed steps in order to mitigate and reduce the Composite Breach Risk Score.

Search Breaches is a function that allows you to search each individual organization that was breached and see more details about the information that was leaked.

3.3. Alerts

Under **Alerts**, you can review any incidents or data leaks that were found by the service as well as follow some mitigation steps which will be found under every alert.

You will be met with two options for managing these alerts:

If you recognize the activity in the alert, you can select the **Archive** option. However, if you do not recognize the activity or have some concerns regarding it, you will have the option to **Open Case** and contact a Resolution Specialist from Sontiq.

Bitdefender Identity Theft Protection alerts monitor:

- **Your Social Security number (SSN).** Smart SSN Tracker intelligently alerts you to all of the names, aliases, and addresses associated with your SSN. If anything looks unfamiliar, it may be an indication of fraud. These smart SSN Tracker Alerts are delivered just like any other alert, which you can view from your Bitdefender Identity Theft Protection dashboard or under the ALERTS section. When you open your Smart SSN Tracker alert, it will show you everywhere and every one your Social Security number is associated with. It will also provide tips and actions you should take if something looks suspicious. For instance, if an unknown alias shows up in your alert, you should notify the credit bureaus immediately.
- **Change of Address.** Criminals typically change the physical address of your mail to gain access to your personal information. They're after your credit card statements, bills, and other financial documents. For this reason, it's very important to monitor for change of address. We monitor and alert you if your mail has been redirected through USPS without your authorization.
- **Court Record.** Our advanced technology has the power to search millions of criminal, court, and public records to make sure your identity is not being used by unauthorized individuals.

- **Fraud.** We can help you place a fraud alert on your credit file. If your identity is at risk, this can prevent thieves from opening new lines of credit in your name. You are promptly notified if your identity is being used to apply for a new credit card, wireless device, utility payments, check reorder, mortgage, or car loan application. This gives you the power to stop fraud attempts rather than having to react after the damage is already done.
- **Identity.** Our online lifestyles leave us more vulnerable than ever to identity theft. We scour thousands of websites, black market chat rooms, blogs, and other data sources to detect the illegal trading and selling of your personal information.
- **Identity Threat.** We keep you updated on major data breaches, identity theft incidents, and new identity theft laws. For example, if a department store has a breach due to theft, your information can be used to open credit cards, apply for loans, and worse.
- **Payday Loan.** Sometimes a criminal will obtain a payday or quick cash loan using your social security number. These loans have incredibly high-interest rates and can really damage your credit and finances.
- **Sex Offender.** Bitdefender keeps a close eye on sex offender registries to monitor for illegal use of your identity. We conduct in-depth searches to find out if a sex offender fraudulently used your personal data as their registration information, or if a sex offender moves into your neighborhood.

3.4. Credit

Under **Credit**, our customers will be able to select a wide range of monitors such as:

- **Credit Score:** simply monitors your credit score, based on the information you have provided for us (credit cards/bank accounts).
- **Credit Report:** presents detailed information about the credit summary as well as history. In the **Credit History** section, you can view your **Two Year Payment History**, **Personal Information**, as well as **Recent Inquiries** or **Creditor Contact Information**.
- **Credit Simulator:** allows you to run a credit score simulation in order to see how you can improve your credit score.

- **Freeze My Credit:** an easy to use, one-click option to contact the desired credit bureau in order to freeze a credit. In addition, it also has an information tab with several FAQs and tips regarding credit freezing.

3.5. Resources

Under **Resources**, you have a wide array of calculators, forms and government resources you can use in order to calculate the best loans, credit cards, how to protect your identity, file a complaint or opt out of telemarketing calls.

3.6. Account

The **Account** tab contains detailed information about you and your account, which can be edited with a simple click.

Under **My Account**, you can choose your contact preferences and edit your personal information.

Under **Protection Plan**, you can review the features of your chosen protection plan.

Under **My Services**, you can review the currently active components from your Identity Theft Protection service.

3.7. Support

The support page is where you'll find yourself able to access frequently asked member questions as well as our 24/7 support phone number.

4. FREQUENTLY ASKED QUESTIONS

4.1. General questions about Bitdefender Identity Theft Protection

What is Identity theft?

Identity theft is a crime where someone has stolen another person's information and then used that personal data in a fraudulent or deceptive manner. Most often, identity theft and identity fraud are committed for financial gain, according to the U.S. Department of Justice. Identity crimes may also be perpetrated by an identity thief trying to avoid legal or criminal actions against their own identity, or who is trying to steal benefits or services that rightfully belong to someone else. Tens of millions of Americans are victims of identity theft every year.

What is the difference between Bitdefender Identity Theft Protection and Bitdefender Digital Identity Protection?

Bitdefender Identity Theft Protection and Bitdefender Digital Identity Protection are not identical. Although some of their functions overlap, such as Dark Web and Social Media monitoring, they target different things. Bitdefender Digital Identity Protection monitors your digital footprint to prevent data breaches and improve your online privacy. On the other hand, Bitdefender Identity Theft Protection focuses on credit monitoring to help you avoid becoming a credit fraud and identity theft victim.

I received an alert from Bitdefender Identity Theft Protection. What should I do?

Some alerts are more urgent than others and may require different actions for you to take. That's why every alert you get also includes What Should I Do? which recommends the next steps for you to take. So you'll always know where your time and attention should be spent.

What is Smart SSN Tracker?

As part of our suite of protection services, Bitdefender Identity Theft Protection monitors your Social Security number (SSN). Smart SSN Tracker intelligently alerts you to all of the names, aliases, and addresses associated with your SSN. If anything looks unfamiliar it could be an indication of fraud.

4.2. Security questions about Bitdefender Identity Theft Protection

What security protocols does Bitdefender Identity Theft Protection enforce for its members?

We utilize 2-factor authentication, requiring members to provide a verification code when they first log in. Bitdefender sends you that code via text, email, or phone, making it much harder for hackers to access your account. It's the best data system protection that an ID monitoring service can use for its networks.

How do you protect the information your subscribers provide?

We operate a risk-based information systems security management program that implements industry-standard best practices for protecting member data.

- Administrative & technical controls include those outlined in PCI DSS v3.2 requirements and ISO 27002 security techniques.
- Sensitive PII is encrypted with the AES symmetric encryption algorithm using 256-bit sized keys.
- Custom master keys are created for all encrypted volumes and any snapshots created from them.

What happens to my information if I cancel my membership?

A member's personal information remains in our system after the account cancellation to facilitate account reactivation. If a user requests to be removed from the system, their information is purged from the database after 180 days.

How does Bitdefender protect itself against cyber fraud?

Our job is to protect customer data from unauthorized access, and we take that responsibility seriously. Here are some of the regulations, standards, and laws with which Bitdefender Identity Theft Protection powered by IdentityForce is required to comply:

- **Payment Card Industry Data Security Standards (PCI DSS):** Industry requirements put forth by the card brands & acquirer banks to safeguard cardholder data. We completed an independent audit for PCI Level 1 in July 2018.

- **Sarbanes-Oxley Act (SOX):** Security of information supporting internal control structures for financial reporting. Although primarily for public companies, several provisions of the Act also apply to privately held companies; for example, the willful destruction of evidence to impede a Federal investigation.
- **Statement on Standards for Attestation Engagements (SSAE) 16:** An auditing standard for service organizations, superseding SAS 70. The latter's "service auditor's examination" is replaced by a "Service Organization Controls" (SOC) report. We completed an independent audit for SOC2 Level 2 in July 2018.
- **State Data Privacy/Breach Notification Laws:** Legislation requiring organizations to notify individuals or entities when there are breaches involving personal information. Additionally, we are required to conform to state laws wherever we have subscribers.

4.3. Stolen identity questions

What should I do if my personal information or identification documents have been stolen?

If somebody has stolen your personal information or identification documents, and you are a Bitdefender Identity Theft Protection subscriber, you can send us an email at bitdefender@identityforce.com and one of our experts will contact you, or you may call our team at 800-399-0710.

What else should credit fraud and identity theft victims do ASAP?

Whether you're a Bitdefender Identity Theft Protection subscriber or not, here are some immediate steps you can take:

1. **Lock down the problem account**
   Contact the financial institution, dispute the charges, and ask to lock or close the account.
2. **Sign up for a credit monitoring service if it's available to you**
   If your information was part of a data breach, there's a one in three chance that your identity has been stolen. Carefully read the data breach alert. If it offers free credit monitoring, sign up.
3. **Read credit card and bank statements to look for other unauthorized charges**

Don't forget to review active, dormant, and infrequently used accounts. If you see anything amiss, contact your financial institution and close your account immediately.

4. **Request a credit report from all three major reporting agencies**
   To assess whether you're a victim of credit fraud or identity theft, request all three types of credit reports at the official site: https://www.annualcreditreport.com/index.action . Use the reports to look for any mystery accounts you don't recognize. And remember, by law, you're entitled to at least one free credit report from each agency per year.

5. **Contact the Federal Trade Commission**
   For credit card fraud, in which only a single account was compromised, an FTC report isn't warranted. To file a report for a stolen identity, visit https://ftccomplaintassistant.gov/ or call 1-877-ID-THEFT (438-4338).

6. **Call your local police department to file a report**
   It's crucial to file a local police report because once it's on record, you're protected against other fraudulent claims. You're also creating a paper trail to show that you're proactively addressing the problem. Even if the police can't investigate the crime or catch criminals online and overseas, your report could help them track down local culprits.

7. **Request fraud alerts from all three major credit report bureaus**
   Fraud alerts notify any institution that pulls your credit report that your identity may be compromised. Alerts also prompt creditors to take an extra step to verify the identity of the person opening the account. Initially, a fraud alert lasts 90 days, but if you have proof that you are a victim of identity theft, the credit bureaus can extend it up to seven years. You can remove this at any time with a written request.

8. **Implement the following preventative security measures**
   a. Create strong passwords & regularly change them.
   b. Shred documents with personal information when disposing them.
   c. Keep personal information (i.e. address, phone number, etc.) off social media sites, as well as any details you use for online security questions.
   d. Avoid carrying your Social Security card in your wallet.

After using Recovery & Restoration services, how do I know if my identity has been restored?

Our team will reach out to you first. We won't close your case until both you and a Restoration representative agree that the existing case has been resolved. If not, the case stays open and we'll keep working to resolve it. If fraudulent activity reappears on a closed case, we'll reopen the case and reactivate our Restoration services, provided your membership is still active.

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.