Bitdefender®

DIGITAL IDENTITY PROTECTION

USER'S GUIDE

Bitdefender Digital Identity Protection

User's Guide

Publication date 11/21/2022

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 Digital Identity Protection as their dedicated software tool for keeping them safe against the rising tide of online data breaches. The information presented in this book is suitable not only for computer literates, but rather it is accessible to everyone.

You will find out how to start taking control of your online privacy by having Bitdefender Digital Identity Protection scan the web for unauthorized leaks of your personal data, monitoring if your accounts are exposed and making it easy to take action well before any disasters strike. 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 Digital Identity Protection and its user interface.

Data Breaches (page 8)

Learn how to take proper care of the protection of your digital identity. Start by understanding what Data Breaches are and how to review them in order to take proper action for the protection of your online privacy.

Getting Help (page 14)

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 DIGITAL IDENTITY PROTECTION

Online privacy and security are some of the main focuses for internet users nowadays. And there are some very good reasons for that. With major data breaches happening more often than not, it is imperative to make sure that your personally identifiable information (PII) is safe and secure.

But what can be classified as personally identifiable information? Traditionally, sensitive information such as the full name, social security number, driver's license, mailing address or credit card information were considered PII. Eventually, less-sensitive info, such as zip codes, IP addresses, or login IDs were also included. Over time, your digital footprint, meaning the data you leave behind as a result of your browsing the internet, might come to include some of these.

Bitdefender Digital Identity Protection represents the private way to online freedom, allowing you to regain control of your digital life. And it requires only your name, most used email address and your phone number. Based on these, it searches on both the Surface Web and the Dark Web for personal information that was exposed publicly.

Bitdefender Digital Identity Protection offers the following:

- **Monitoring and detection services:** it monitors more than 100 personally identifiable information such as SSN, credit cards or home address, and displays all data found about your online footprint.

  > **Note**
  > Bitdefender does not store or process personally identifiable information. Only references to potential data breaches are kept, without including sensitive data.

- **Real-time alerts:** You receive notifications about data breaches and exposed data in Dark Web, personal information in Surface Web and potential impersonators you on social media.
- **Solutions:** Our service suggests clear actions required to solve issues and provide reminders if an issue is not solved entirely. It can also provide instructions on how to remove the personalized ads, export your data, or turn off the tracking.

2. GETTING STARTED

2.1. Activate Digital Identity Protection

Activate the Bitdefender Digital Identity Protection subscription after your order is placed and paid.

1. Open the confirmation email received shortly after completing your order and click on **GET STARTED**.
2. You will be redirected to https://central.bitdefender.com.
   Sign in with your Bitdefender Central account. If you don't have an account, choose to create one.
3. After signing in, the subscription will automatically be attached to your Central account and will trigger the onboarding process.

Alternatively:

- access the **My Subscriptions** panel from Central, located on the left side of the window, and click **+ Activate with code**.
- type in the 10 digit-key found in your confirmation email and press **ACTIVATE**.
- if prompted, select how you would like to use the code, then click on **ACTIVATE**.

2.2. Configure Digital Identity Protection

1. Go to https://central.bitdefender.com/ and sign in to your account.
   If you don't already have an account, click on **CREATE ACCOUNT**, then type your full name, an email address and a password.
2. Select the Digital Identity Protection panel.
   A welcoming screen is displayed.
3. Click **BEGIN**.
4. You will now be informed on what information you need to provide. Your data will always be encrypted and secured.
   Click **NEXT**.
5. Type your first name, middle name (if any) and last name in their corresponding boxes, then click **NEXT**.

6. Type your email address, then click **NEXT**.
   Make sure it is a valid email address you can access.
7. A security code is sent to the address you provided.
   Open your email, copy the code and paste it in its corresponding field.
   After that, click **CHECK**.
8. Select your country and enter your phone number, then click **NEXT**.
9. You should receive a security code shortly after that.
   Enter the code, then select **CHECK**.
10. After the initial check is performed, click **FINISH**.

> **Note**
> You will be informed if any breaches, personally identifiable information or potential impersonation attempts are discovered during this first check.

Bitdefender Digital Identity Protection is now configured.

2.3. Review your Digital Footprint, Data Breaches and possible Impersonations

After you complete the configuration, Bitdefender Digital Identity Protection performs an online check to discover potential impersonations, data breaches and personally identifiable information on the Open Web. We recommend reviewing every piece of info included in the **DIGITAL FOOTPRINT**, **DATA BREACHES** and **IMPERSONATION CHECK** tabs.

- Reviewing your Digital Footprint (page 7)
- Reviewing Data Breaches (page 8)
- Reviewing possible Impersonations (page 9)

2.4. Improve your check-up

We use the data you provide to monitor the Surface Web and Dark Web to detect any activity that might affect your privacy or your personal brand reputation.

If you would like to add another email address or another phone number, click ⊕, then click on **ADD EMAIL ADDRESS** or **ADD PHONE NUMBER** and follow the instructions.

3. DASHBOARD

The Dashboard aggregates information included in the **DIGITAL FOOTPRINT**, **DATA BREACHES** and **IMPERSONATION CHECK** sections.

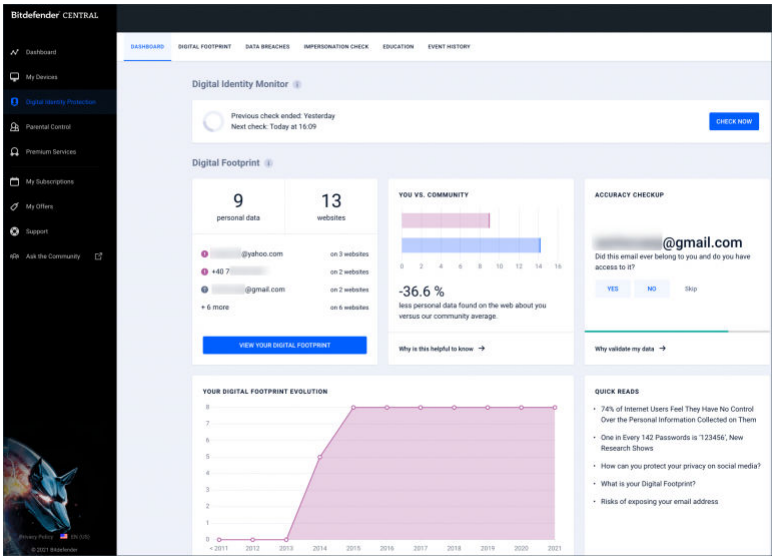
It includes the following:

- Your exposed data and their web sources
- The average amount of exposed data for the entire community
- Your Digital Footprint evolution
- Privacy-related content
- Data Breaches
- The average number of data breaches inside the community

3.1. Digital Identity Monitor

Using only accurate information Bitdefender's system looks for new personal data exposed on the Open Web and Dark Web and scans all the major Social media platforms for any signs of an impersonation attempt.

Click on **CHECK NOW** to perform an online scan.



4. DIGITAL FOOTPRINT

Your personally identifiable information and their sources appear here. It is up to you to evaluate if having the information public on the web is a threat.

Our AI-driven monitor relies heavily on correct data to detect new threats, so please tell us if the information is accurate or inaccurate.

Once you confirm a piece of information is yours, we add it to our monitoring system and improve the chances of discovering other ones in the future.

4.1. Reviewing your Digital Footprint

To review your digital footprint:

1. Go to the **DIGITAL FOOTPRINT** tab.
2. Information that has not been verified yet will appear with the text **Verify** on the right side. Click **Verify**, then select Yes or No, depending on the case.

> **Note**
> Every piece of information confirmed is added to our monitoring algorithm, improving the results displayed by our services. Information that is dismissed will no longer be displayed. However, it will still remain available on the web.

5. DATA BREACHES

Breaches occur when hackers manage to bypass a company's security measures and obtain your personal information, to sell it on the dark web. Typically, cybercriminals target login data, personally identifiable information (PII), medical records, and banking-related details.

Any organization or service can fall victim to a data breach, but those with a large consumer base make more attractive targets. Breaches commonly include names, email addresses, usernames, passwords, postal addresses, phone numbers, social security numbers (SSN) and credit card data (number, expiration date, CVV).

5.1. Reviewing Data Breaches

To review your data breaches:

1. Go to the **DATA BREACHES** tab.
2. Under some entries, you will find a list of actions required for securing your account. After performing an action, click the box next to it in order to confirm.
   If you're not sure about how to perform a task, you can always click on the link included in the task description and you'll be redirected to a page where you'll find all the necessary steps.
   Not all breaches can be dealt with in this manner. Some of them, such as **Collection #1**, won't include steps. Instead, you will be redirected to articles available online where you can find more help.

   Note
   Bitdefender does not store or process personally identifiable information. Only references to potential data breaches are kept, without including sensitive data.

6. IMPERSONATION CHECK

Criminals known as “pretexters” use the art of impersonation in many ways, playing the role of a trusted individual to deceive their victims and gain access to sensitive information. The practice of “pretexting” is defined as presenting oneself as someone else to manipulate a recipient into providing sensitive data such as passwords, credit card numbers, or other confidential information.

Bitdefender Digital Identity Protection monitors 25 Social Media platforms and notifies you instantly if it finds a profile that could be an impersonation attempt.

6.1. Reviewing possible Impersonations

The **IMPERSONATION CHECK** tab is where all possible attempts will be displayed. For each detection, you can choose one of three possibilities:

- It is an impersonation attempt
- It is your own profile
- It is a different profile

Depending on the choice, Bitdefender Digital Identity Protection will recommend specific steps in order to deal with the issue. Every time you complete a step, you can mark it as **Done**.

7. EDUCATION

The Education tab serves as a knowledge base where the user can find more information on how to protect their digital identity.

Articles listed here can be sorted into several categories:

- Breaches
- Exposures
- Impersonation Check

To access the full version of an article, click on its corresponding **Read more** link.

8. EVENT HISTORY

The Event History section is the means by which we communicate constantly with our users. It represents a chronologically ordered list of events regarding the protection of your Digital Identity.

Besides newly detected threats (if any), you can return to this page for valuable advice on how to properly conduct yourself online, to increase the chances of not dealing with privacy issues.

In the Event History section, you can find the following information:

- Actions performed
- Service updates
- Data Breaches

9. FREQUENTLY ASKED QUESTIONS

Why is online privacy so important nowadays?

Online privacy means protecting your private and financial data from cybercriminals. Such personally identifiable information has great value on the Internet and once these details are leaked, your money is no longer safe. You will need a reliable service for continuous identity protection and monitoring to make sure your private data always stays private.

What is my digital footprint?

Your digital footprint is your entire online activity. Each login into your social accounts, each bank transaction, everything that you purchase online can be exposed to data breaches. You need to be aware at all times about the way your private and financial data is stored and handled - and take the necessary steps to protect it.

What are data breaches and how do they impact my personal accounts?

Data breaches are security incidents when private data is leaked to unsafe environments. These can be exploited by cybercriminals all around the globe to gain access to your online identity. Data breaches can impact your credit score, medical insurance, college funds, or even your retirement account.

How can Bitdefender Digital Identity Protection help with my online privacy?

Bitdefender Digital Identity Protection continuously monitors your personal information and alerts you in real time in case of a data breach. This way you can change your passwords and secure your accounts to prevent any financial loss or social media impersonations.

Where does Bitdefender Digital Identity Protection look for data?

Bitdefender Digital Identity Protection looks for data on the surface web (social media networks, posts, blogs, forums, data brokers, publications, offline databases) but also on the Dark Web marketplaces, where cybercriminals trade information gathered from data breaches.

How is Bitdefender Digital Identity Protection different from other (free) services?

Bitdefender Digital Identity Protection has unparalleled capabilities of monitoring considerable volumes and higher quality of data from the Dark

Web. The information from the Dark Web is curated and de-duplicated so we can reduce false positive alerts.

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

How can I use the service? Do I have to download anything?

You do not have to download anything, as Bitdefender Digital Identity Protection is an online service. You gain access to a web dashboard where you can monitor all your personal accounts in real-time.

How can I receive alerts for future data breaches?

To receive alerts for future data breaches you simply sign up for e-mail alerts from your web dashboard and you will start to receive privacy alerts and security reports from Bitdefender Digital Identity Protection.

10. GETTING HELP

10.1. 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.

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

10.2. 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
- 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.

10.2.1. 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/support/consumer.html.

10.2.2. 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

10.2.3. 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/.

10.3. 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/

10.3.1. 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.