Bitdefender® CONSUMER SOLUTIONS

Password Manager
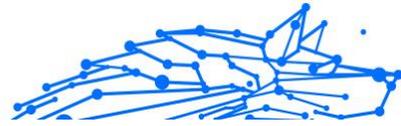
Bitdefender Password Manager

User's Guide

Publication date 09/06/2023
Copyright © 2023 Bitdefender

Legal Notice

Bitdefender®

Table of Contents

ABOUT THIS GUIDE

Purpose and Intended Audience

This guide is intended to all Bitdefender users on all supported operating systems (Windows, MacOS, Android, iOS) who have chosen Bitdefender Password Manager as their go-to password management tool. The information presented in this book is suitable not only for computer literates, but it serves as an accessible and friendly guide to everyone.

This guide will help you find out how to make the best of our ultra-secure and feature-rich password manager, by discussing in detail all of its features and functionalities.

We wish you a pleasant and useful lecture.

How to Use This Guide

This guide is organized around several major topics:

Get started with Bitdefender Password Manager and the installation process.

Learn how to use Bitdefender Password Manager and all of its features.

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.
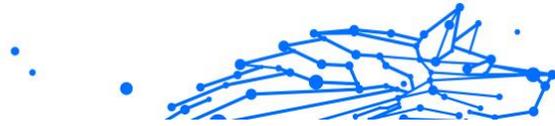
Appearance	Description
sample syntax	Syntax samples are printed with monospaced characters.
https://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
documentation@bitdefender.com	Email addresses are inserted in the text for contact information.
About this 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 PASSWORD MANAGER

Bitdefender Password Manager is a multi-platform service designed to help users store and organize all of their online passwords. It is built with the strongest known cryptographic algorithms for the highest level of safety and digital security. It works as a browser extension and mobile app solution for identity and password management, banking and all other types of sensitive information across devices.

Bitdefender Password Manager can auto-save, auto-fill, automatically generate and manage your passwords for all websites and online services with the help of a single Master Password, making your overall digital identity much easier to manage.

1.1. Security and how it works

Behind the Bitdefender Password Manager software stand some of the latest cryptographic algorithms which assure the highest data security users can hope for, such as AES-256-CCM, SH512, BCRYPT, HTTPS and WSS protocols for data transmission. All data involved is at all times encrypted and decrypted locally. This makes it such that only the account holder alone can have access to the information stored within the account, as well as to the Master Password that is used to access and subsequently make use of the data in question.

1.2. Password Manager Trial & Paid versions

The Trial version of Bitdefender Password Manager works by all accounts identical to the Paid version of the product, but its availability will expire after the trial period.

> **ⓘ** Note
> Note that the Paid version of the product, whilst it can be purchased as a purely standalone product, unlimited access to Password Manager is included within the Bitdefender Premium Security and Bitdefender Ultimate Security subscriptions.

2. GETTING STARTED

2.1. System Requirements

You may use the latest version of Bitdefender Password Manager only on devices running the following operating systems:

❍ **For PC users:**

  ❍ Windows 7 with Service Pack 1

  ❍ Windows 8

  ❍ Windows 8.1

  ❍ Windows 10

  ❍ Windows 11

❍ **For macOS users:**

  ❍ macOS 10.14 (Mojave) and later macOS operating systems

  > **Note**
  > Note that System Performance may be affected on devices that have old generation CPUs.

❍ **For iOS users:**

  ❍ iOS 11.0 or later iOS operating systems

❍ **For Android users:**

  ❍ Android 5.1 and later Android operating systems

  > **Note**
  > ❍ Fingerprint unlock feature is supported on **Android 6.0** and later.
  > ❍ Autofill feature is supported on **Android 8.0** and later, compatible with iPhone, iPad and iPod touch.

2.1.1. Software Requirements

To be able to use Bitdefender Password Manager and all its features, your Windows or macOS devices need to meet the following software requirements:

❍ **Microsoft Edge** (based on Chromium 80 and later)

❍ **Mozilla Firefox** (version 65 or later)

❍ **Google Chrome** (version 72 or later)

❍ **Safari** (version 12 or later)

> **ⓘ Note**
> The Sofware Requirements are not applicable for Android and iOS.

> **✕ Warning**
> Failure to meet the System Requirements presented above will result in either the inability of installing Bitdefender Password Manager or the malfunctioning of the product.

2.2. Installation

This chapter will guide you on how to install Bitdefender Password Manager to both the web browsers on your Windows PC and macOS, as well as on your mobile Android or iOS devices.

> **! Important**
> Prior to the installation, make sure that you have a valid Password Manager subscription in your Bitdefender Central account so that this browser extension can retrieve its validity from your account.
>
> Active subscriptions are listed in the **My Subscriptions** section within Bitdefender Central.

2.2.1. Installing on Windows and macOS devices

Unlike most desktop applications and software which need to be installed and set up on these devices, Bitdefender Password Manager comes as a browser extension - also called an add-on - that can be quickly added and enabled to your preferred browser.

The currently supported browsers for the product are the following: **Google Chrom**e, **Mozilla Firefox**, **Microsoft Edge**, and **Safari**.

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 **My Devices** on the left sidebar of the screen.

3. In the **My Devices** section, proceed by clicking on **+ Add Device**.

4. This action will prompt a new window to pop up. Choose **Password Manager** in the selection screen.

5. Choose **This Device**.
    If you are looking to install on a different device, select Other devices. You can then email a download link to the respective device or directly copy the URL for the installation.

6. Next choose on which browser you want to install the Password Manager extension.

7. Each corresponding button will redirect you to the browser's Extensions Store. From there, simply follow the instructions on screen as shown below:

    Microsoft Edge

    ❍ Click the **Get** button

    ❍ Click **Add extension** in the prompt that appears on screen

    Google Chrome

    ❍ Click the **Add to Chrome** button

    ❍ In the confirmation box, click **Add extension**

    Mozilla Firefox

    ❍ Click the **Add to Firefox** button

    ❍ Click the **Install** button in the upper right corner of the screen

    Safari

    ❍ Click the **Get** button, then click **Install**

    ❍ Open Safari and select **Preferences** in the top menu bar

    ❍ In the Preferences window, click the **Extensions** tab

    ❍ Select the checkbox next to Password Manager to enable it

Once you have followed these steps, set a strong master password, then press the **Save Master Password** button after you read and agree with the **Terms and conditions**.

> ⚠️ **Important**
> Note that you will require this Master Password to unlock all the passwords, credit card information and notes saved in Bitdefender Password Manager. This is essentially the key that allows the owner to use this product.

> ❌ **Warning**
> Upon creating the Master Password, you will receive a **24-digit recovery key**. Make a note of your recovery key in a safe place and don't lose it. This key is the only way to access your passwords saved in Password Manager in the event that you happen to **forget the Master Password** previously set up for your account.

> ❍ You can press **Close** when done.

2.2.2. Installing on Android devices

The easiest method of installing Bitdefender Password Manager for Android phones and tablets is to download the application directly from Google Play.

Installing the Bitdefender Password Manager app can also be done through your Bitdefender Central account:

1. On your Android mobile device sign in to your Bitdefender Central account by accessing https://login.bitdefender.com/central/login.

2. Select **My Devices** on the left sidebar of the screen.

3. In the **My Devices** section, proceed by clicking on **+ Add Device**.

4. This action will prompt a new window to pop up. Choose **Password Manager** in the selection screen.

5. Choose **This Device**.
   If you are looking to install on a different device, select **Other devices**. You can then email a download link to the respective device or directly copy the URL for the installation.

6. You will be redirected to Google Play. Tap **Install** to download Bitdefender Password Manager on Android.
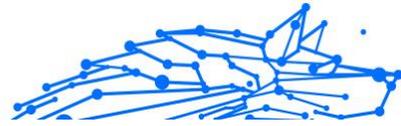
7. Once the download is completed, open the ⓥ Password Manager application.

8. If you are not automatically logged in to your account, sign in using your username and password.
   Once you have followed these steps, set a strong master password, then press the **Save Master Password** button after you read and agree with the **Terms and conditions**.

   ⚠ Important
   Note that you will require this Master Password to unlock all the passwords, credit card information and notes saved in Bitdefender Password Manager. This is essentially the key that allows the owner to use this product.

   ✖ Warning
   Upon creating the Master Password, you will receive a **24-digit recovery key**. Make a note of your recovery key in a safe place and don't lose it. This key is the only way to access your passwords saved in Password Manager in the event that you happen to **forget the Master Password** previously set up for your account.

   ❍ You can press **Close** when done.

9. Create a **4-digit PIN**, so if you switch to another app and then return to Password Manager, you won't have to re-enter the master password you set up previously. If available, you can also enable face recognition or fingerprint authentication.

10. Tap on **Enable Autofill** to configure Android autofill settings.

    ⓘ Note
    If you skip this step, you can enable and customize the Android autofill features at a later time by following the instructions available at Intelligent Autofill (page 19).

11. You will be met by a list of apps that can autofill passwords.
    - Select **Password Manager** and then the device will prompt you to confirm that you trust this app.
      Tap **OK**.
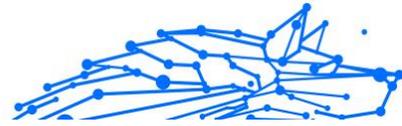
12 Enter the PIN you set up in **step 9** to confirm this action.
.

The installation on your Android device is now complete.

2.2.3. Installing on iOS devices

The easiest method of installing Bitdefender Password Manager for iOS and iPadOS devices is to download the application from the Apple App Store.

Installing the Bitdefender Password Manager app can also be done through your Bitdefender Central account:

1. On your iPhone or iPad sign in to your Bitdefender Central account by accessing https://login.bitdefender.com/central/login.

2. Select **My Devices** on the left sidebar of the screen.

3. In the **My Devices** section, proceed by clicking on **+ Add Device**.

4. This action will prompt a new window to pop up. Choose **Password Manager** in the selection screen.

5. Choose **This Device**.
   If you are looking to install on a different device, select **Other devices**. You can then email a download link to the respective device or directly copy the URL for the installation.

6. You will be redirected to **App Store**. Tap the cloud icon with an arrow pointing down to download Bitdefender Password Manager for iOS.

7. Once the application is installed, open it and check the small box on the screen. Select **Continue** after you read and agree with the **Subscription Agreement**.

8. If you are not automatically logged in to your account, sign in using your username and password.
   Once you have followed these steps, set a strong master password, then press the **Save Master Password** button after you read and agree with the **Terms and conditions**.

> **! Important**
> Note that you will require this Master Password to unlock all the passwords, credit card information and notes saved in Bitdefender Password Manager. This is essentially the key that allows the owner to use this product.

> **✕ Warning**
> Upon creating the Master Password, you will receive a **24-digit recovery key**. Make a note of your recovery key in a safe place and don't lose it. This key is the only way to access your passwords saved in Password Manager in the event that you happen to **forget the Master Password** previously set up for your account.
>
> ❍ You can press **Close** when done.

9. Create a **4-digit PIN**, so if you switch to another app and then return to Password Manager, you won't have to re-enter the master password you set up previously. If available, you can also enable face recognition or fingerprint authentication.

The installation on your iOS / iPadOS device is now complete!

3. SHARED PLAN

Bitdefender Password Manager Shared Plan enables multiple users to access and utilize the same subscription. It provides a centralized approach to software access, administration, and support.

❍ The person in charge of the shared subscription plan, known as the Plan Manager, can share the service among the members.

❍ Each member gets their own unique **Bitdefender Central** account linked to their email address and access to the Bitdefender Password Manager service.

3.1. Sharing Bitdefender Password Manager with multiple users

Inviting members

To add one or multiple users to the shared subscription, the plan manager must follow these steps:

1. Log in to your Bitdefender Central account at https://central.bitdefender.com/

2. Go to the **My Subscriptions** menu located on the left side of the page.

3. Choose **Invite member** in the **Bitdefender Password Manager Shared Plan** panel.

4. Enter the email of each person you wish to share your subscription with, then click on **Send**. A maximum of 3 members can be added at once.

5. Setup instructions are emailed right away to the new members. Click on **Close** to exit the confirmation window.
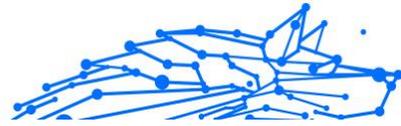
> ⓘ **Note**
> Members have 24 hours to accept your invite once it's emailed to them.

- ❍ Invited members will appear with the status "Invited".
- ❍ You will see them as "Active" members after they accept the invitation. You are also notified by email of each accepted invitation.

Removing members

Bitdefender Password Manager Shared Plan access is lost for members who are removed. When the plan manager decides to remove a subscription member, the member receives an email notification. For the following 30 days, the ex-member is switched to a 30-day Bitdefender Password Manager **trial version** with full capabilities. The service will then be turned off.

The plan manager can eliminate users from the shared plan in the following way:

1. Log in to your Bitdefender Central account at https://central.bitdefender.com/

2. Go to the **My Subscriptions** menu located on the left side of the page.

3. In the **Bitdefender Password Manager Shared Plan** panel click on **Manage**, then choose **Edit members** in the menu.

4. Click the **Remove** button to take a member off the shared plan.

5. Choose **Yes**, remove member then click the **Finish editing** button for the changes to take effect.

> ⓘ **Note**
> When a member is deleted from the shared plan, their status is changed to **Pending removal** until they are completely eliminated.

Accepting an invitation

You will receive an email when someone invites you to become a subscription member for Bitdefender Password Manager Shared Plan. You have 24 hours to accept an invite once it's sent to you.

To accept the invite and gain access to the password manager features, the user must follow these steps:

1. Open the email you received titled **[Start using your Bitdefender subscription as a Member]** and click the **ACTIVATE IN CENTRAL** button.

2. The Bitdefender Central page will then open in your browser.

   ❍ If you already have a Bitdefender user account associated with the email where the invitation was sent, **sign in** to claim your shared subscription.

   ❍ If you don't have a Bitdefender user account, click on **Create one** and sign up with the same email where the invitation was sent to claim your shared subscription.

      ❍ Enter your full name

      ❍ Enter your email address

      ❍ Enter your password

      ❍ Click the **Create Account** button and you will be signed.

3. After signing in, click on **Get started** on the welcome screen that informs you that your Bitdefender Password Manager subscription is now active.

4. Follow the on-screen steps also described in Installation (page 5).

> **ⓘ Note**
> The plan manager's email is displayed in your Bitdefender Central account at the top of the Password Manager menu and on the subscription card, under My Subscriptions.
>
> If you need assistance with the shared plan, please get in touch with them.

4. IMPORTING & EXPORTING YOUR PASSWORDS

Bitdefender Password Manager is built in such a way as to efficiently facilitate communication and data transfer with external sources, platforms and software tools. This is the core reason why the very frequently encountered need of importing or exporting passwords into or out of Bitdefender Password Manager can be satisfied with ease.

4.1. Compatibility

Bitdefender Password Manager can seamlessly transfer data from the following list of applications:

- **1Password**
- **Bitwarden**
- **Bitdefender Password Manager**
- **ByePass**
- **Chrome browser**
- **Claro**
- **Dashlane**
- **Edge browser**
- **ESET Password Manager v2**
- **ESET Password Manager v3**
- **StickyPassword**
- **Watchguard**
- **Firefox browser**
- **Gestor de contraseñas – Claro**
- **Gestor de contraseñas – SIT**
- **Gestor de contraseñas – Telnor**
- **KeePass 2.x**
- **LastPass**
- **Panda Dome Passwords**

❍ **PassWatch**

❍ **Saferpass**

❍ **SFR Cybersécurité**

❍ **SIT**

❍ **F-Secure**

❍ **Telnor**

> ⓘ Note
>
> If the name of the browser or password manager tool from which you are trying to transfer data files is not mentioned in the list provided above, you can follow our online guide on how users can edit a CSV file from unsupported password managers so that you can import your information into **Bitdefender Password Manager**: https://www.bitdefender.com/consumer/support/answer/2472/

This transfer of data between Bitdefender Password Manager and other account management software can be done through the following data formats:

CSV, **JSON**, **XML**, **TXT**, **1pif** and **FSK**.

4.2. Importing into Password Manager

Bitdefender Password Manager allows you to easily import passwords from other password managers and browsers. If you are currently looking to switch to Bitdefender Password Manager from another password managing service, you have most likely stored a considerable amount of credentials such as usernames, passwords, and other login data required for all your accounts.

Now that you've chosen Bitdefender Password Manager, you will be looking to import that saved data into it.

Here is how to import your stored information from other apps and web browsers into Bitdefender Password Manager, **regardless of the operating system** on which you have chosen to install this product:

1. Click the Password Manager icon in your web browser (on Windows or macOS) or launch the Password Manager application (on Android or iOS). If prompted, enter your Master Password.
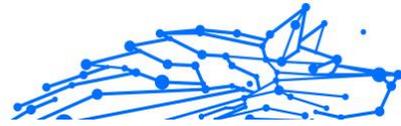
2. Open the Password Manager ≡ menu to expand the sidebar on the left and click the ⚙ **Settings** menu item.

3. Scroll down to the **Data** section and click on the **Import Data** option.

4. Use the drop-down menu to select the name of the password manager app or browser you want to import your accounts from. Input your Master Password in the corresponding field, then click on **Choose File**.
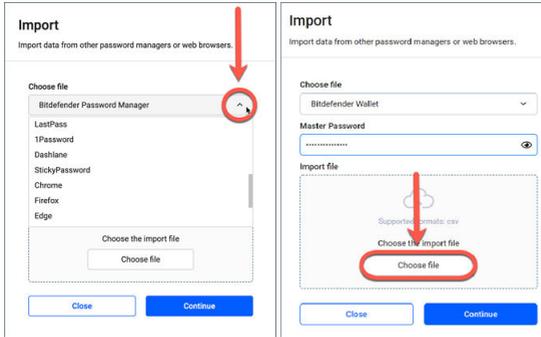
5. Browse through your folders to find the location in which you have saved the file containing your usernames and passwords, exported from your other password manager or web browser, then press **Continue**.

Once imported, your passwords will then be accessible on all devices where Bitdefender Password Manager application or browser extension is installed.

4.3. Exporting from Password Manager

Bitdefender Password Manager allows you to easily export your saved passwords (including account login credentials, secure notes, etc.) into a CSV (comma-separated values) file or an encrypted file if you ever wish to switch to another password manager service, so that your departure from Bitdefender Password Manager will not be a difficult process.
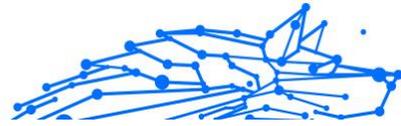
> **Important**
>
> A CSV file is **not** encrypted and contains usernames and passwords in plain text format, meaning your private information can be read by anyone having access to your device. We therefore recommend you follow the instructions below on a trusted device.

Here is how you can export your data from Bitdefender Password Manager:

1. Click the Password Manager icon in your web browser (on Windows or macOS) or launch the Password Manager application (on Android or iOS). If prompted, enter your Master Password.

2. Open the Password Manager menu to expand the sidebar on the left and click the ⚙ **Settings** menu item.

3. Scroll down to the **Data** section and click on the **Export Data** option.

4. Now you should be prompted with the following two options:

   ❍ **CSV**

   ❍ **Password-protected files**

   Select your preferred option, then input your Master Password, and click the **Export data** button.

   > **Note**
   >
   > If you pick the password-protected file option, you will be asked to encrypt the data containing the accounts list with a password, so this way only you would be able to access it if needed.

5. Your web browser/app will proceed by saving a file named Bitdefender Password Manager_exported_data_current-date to your system in the default download folder. It contains all your data stored in Bitdefender Password Manager.

After exporting your data, you can upload it to the password manager of your choice.

5. FEATURES & FUNCTIONALITIES

This chapter will take you through all features and functionalities of Bitdefender Password Manager, explaining their usefulness and how to operate them most efficiently.

5.1. Password Handling

5.1.1. Password Generator

The golden rule in regards to online security is to always use unique random passphrases for every service that requires account creation. Password reuse across multiple platforms is the number one reason behind identity theft and losses associated with hostile account takeover.

This feature helps users with generating secure, complex, and unique passwords for every new account they create anywhere online. This eliminates the need for users to come up with strong passwords on their own or being careful not to reuse the same password for multiple accounts.

The ⊚ **Password Generator** can be accessed through the tab on the top of the Password Manager interface.

The generator can be set to return passwords **between 4 and 32 characters**.

You can also specify the types of characters that should or should not be present in the randomly generated password by checking or unchecking the corresponding tick boxes. **(Lowercase, Uppercase, Numbers, Special)**

By pressing the ↻ button to the right of the displayed password, the generator will change the suggested password.

To use the displayed password, press **Use password**, action which will save the string of characters to your clipboard.

> ⓘ Note
> Your previously generated passwords will be temporarily stored in Password history, which can be accessed through the **Password history** button.

5.1.2. Password Capturing

With this feature within Password Manager, you will be prompted to store all of your new passwords immediately after creating them. Password Manager will prompt users to store their newly created passwords, so that they may be added to the ultra-safe environment provided by Bitdefender right away.

5.1.3. Intelligent Autofill

Bitdefender Password Manager can be set up in such a way that it can autofill your login credentials and most importantly passwords. Proprietary algorithms can detect and pre-fill credentials on previously visited websites, saving the users' time every time they log in to a service.

1. On Windows or macOS, click on the 🛡 **Password Manager** icon in your web browser.
   On Android or iOS, launch the 🛡 **Password Manager** application.
   If prompted, enter your Master Password.

2. Open the Password Manager menu ▤ to expand the sidebar on the left and click the ⚙ **Settings** menu item.

3. Click on **Device Settings**.

4. Here you will notice a button displaying either **Disable Auto-Fill** or **Enable Auto-Fill**. This setting controls the operating state of the intelligent autofill feature.

5.1.4. Security Report

The Security Report is a tool that will generate reports based on a number of features meant to bolster your digital security. It will let you know if a password requires your immediate attention by determining its level of security. It will detect password duplicates and prompt you to change them accordingly, avoiding the dangers of recycling the same passwords for multiple accounts.

The report will concentrate on providing you with information on your overall password hygiene: this refers to duplicate passwords, weak or otherwise leaked passwords or email addresses.

This is done by comparing the list of encrypted hashes from Troy's webpage locally on your device to check if it contains the corresponding

hashes of your passwords. If a match is to be found, you will be notified so as to encourage you to consequently change your passwords and other login credentials.

To access the **Security Report**, enter the Password Manager interface and select its corresponding ⬚ button in the top bar.

5.1.5. Sync Across Other Platforms

Saving your passwords once into Bitdefender Password Manager will enable you to store and securely access them on all your Windows, Mac, Android or iOS devices from Chrome, Safari, Firefox and Edge or inside mobile apps.

> ⓘ Note
> Bitdefender is also equipped with an **offline mode** to access your passwords, in the event that you happen to not have access to the internet. This makes your passwords accessible at all times and from anywhere.

5.1.6. Deleting an entry

To delete saved passwords first press the ✎ edit icon next to the entry you want to remove, located in the ⚇ **Accounts** tab. Scroll down then choose **Delete**. When asked if you are sure you want to remove the account select **Remove**.

5.2. Account Handling

5.2.1. Authentication

The Authentication into Bitdefender Password Manager is done through the **PIN** set up in the installation process of the product. (Note that the **Auto-Lock** feature will lock the password manager or logout after a period of inactivity at browser level or closing the mobile app)

Additionally, it can also be done through the use of biometrics, if available, such as **Fingerprint** or **Face unlock**.

To **enable or disable** biometry-based authentication:

1. On Windows or macOS, click on the 🛡 **Password Manager** icon in your web browser.
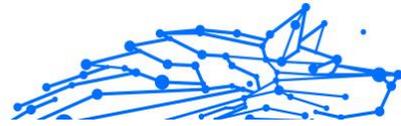
On Android or iOS, launch the 🛡 **Password Manager** application. If prompted, enter your Master Password.

2. Open the Password Manager menu ▤ to expand the sidebar on the left and click the ⚙ **Settings** menu item.

3. Click on **Device Settings**.

4. Here you will notice a button displaying either **Disable biometry** or **Enable biometry**. This setting controls the operating state of the biometry-based authentication feature.

5.2.2. Master Password Reset

⚠ **Important**
The **Change Master Password** feature is not available on mobile devices. The only way you can change or recover your master password is via the Bitdefender Password Manager browser extension on a Windows PC or a macOS device.

Here's how to change your Master Password as a precautionary measure and create a new one in Bitdefender Password Manager:

1. Once you have the browser extension installed, click the 🛡 **Password Manager** icon in your web browser toolbar.

2. Enter your current master password to unlock the vault.

⚠ **Important**
If you do not remember the current master password, click the **I've forgotten my password** option on the same screen. Enter the **24-digit Recovery Key** provided during the initial Bitdefender Password Manager setup, then type a new master password. **If you forget or misplace** both the Master Password and the **Recovery Key**, as a last resort, **contact a Bitdefender representative to help reset your account**. Resetting your account will erase all your data and passwords saved in Bitdefender Password Manager.

3. Open the Password Manager menu ▤ to expand the sidebar on the left and click the ⚙ **Settings** menu item.

4. Click on the **My account** button in the **Account** section.

5. A window with information about your Password Manager subscription will be displayed.

Click on the **Change Master Password** button.

6. You'll be redirected to a new window where you can choose a new master password. Enter your current master password, then type a new master password. The new master password must contain a minimum of 8 characters, at least one lowercase letter, one uppercase letter, and one number.

7. Press the **Change** button when you're done.

8. Wait a few moments until Bitdefender resets the old master password. Do not exit your web browser!

9. Next, you are provided with a new **24-digit recovery key**. Make a note of the recovery key in a safe place and **don't lose it**. This key is the only way to access your passwords saved in Password Manager in case you forget the master password.
   Press **Close** when you're done.

10 You will be logged out of Bitdefender Password Manager.
·   To unlock the vault, use the new master password you just set.

5.3. Other functionalities

5.3.1. Identities management

This feature allows users to store multiple identities and lets Password Manager automatically fill in details in web forms before making a purchase in a quick, easy and secure manner.

Like everything else in Password Manager, all sensitive data contained within these stored identities is encrypted and available only to the user's device.

To add an identity to Password Manager:

1. On Windows or macOS, click on the 🛡 **Password Manager** icon in your web browser.
   On Android or iOS, launch the 🛡 **Password Manager** application.
   If prompted, enter your Master Password.

2. Open the Password Manager menu ▤ to expand the sidebar on the left and click the 🆔 **Identities** menu item.

3. Press on the **Add Identity** button at the bottom.

4. Complete the details you want stored then press **Save**.

5.3.2. Credit Card management

This feature allows you to save and fill credit card details for easier, faster and more secure shopping.

To add a credit card to Password Manager:

1. On Windows or macOS, click on the ⛨ **Password Manager** icon in your web browser.
    On Android or iOS, launch the ⛨ **Password Manager** application.
    If prompted, enter your Master Password.

2. Open the Password Manager menu ▤ to expand the sidebar on the left and click the ▦ **Credit cards** menu item.

3. Press on the **Add Identity** button at the bottom.

4. Complete the details you want stored then press **Save**.

5.3.3. Secure Me

The Secure Me feature allows you to remotely log out or delete browsing history of your computer, tablet or mobile device. If you're sharing a device with other people, we strongly recommend you turn this feature on.

To locate and enable this feature:

1. On Windows or macOS, click on the ⛨ **Password Manager** icon in your web browser.
    On Android or iOS, launch the ⛨ **Password Manager** application.
    If prompted, enter your Master Password.

2. Open the Password Manager menu ▤ to expand the sidebar on the left and click the ⏻ **Secure Me** menu item.

3. Press on the **Secure all sessions** button.
    If you are looking to secure only a particular device, look for it in the list of devices on which Password Manager is installed or enabled on a specific browser.

5.3.4. Notes

Secure Notes is a feature that acts just like a secret notebook where you can store sensitive data, sort it and use color coding to better visualize it. Not only does it keep information tidy, but you also keep it safe and secure.

To locate and enable this feature:

1. On Windows or macOS, click on the 🛡 **Password Manager** icon in your web browser.
    On Android or iOS, launch the 🛡 **Password Manager** application.
    If prompted, enter your Master Password.

2. Open the Password Manager menu ☰ to expand the sidebar on the left and click the 🗒 **Notes** menu item.

3. Press on the ⬜ **Add note** button.
    Once you have written down the information you want to safekeep, press **Save**.
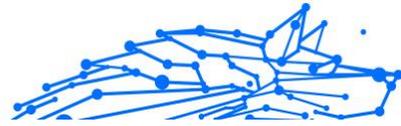
6. FREQUENTLY ASKED QUESTIONS

Some common questions about Bitdefender Password Manager tend to recur. We have the answers! Here you can learn more about your Bitdefender account, importing passwords, data security protocols, and other topics important to our customers.

General questions about Bitdefender Password Manager

How do I stop the Password Manager pop-up in my Bitdefender security solution?

The Password Manager notification displayed by Bitdefender Total Security, Internet Security, and Antivirus Plus in August 2022 can be dismissed by clicking the "x" button. The "Manage your passwords with Bitdefender Password Manager" window will randomly reappear a couple of times before disappearing forever. You can opt out of this promotional message by toggling **Recommendation notifications** to the off position in Bitdefender Settings.

What happens when Bitdefender Password Manager expires?

Once your Password Manager subscription expires and is no longer active, you will have a maximum of 90 days to export your passwords. Your passwords will be backed up for another 30 days. During those 90 days, you will only be able to export your data. You cannot continue to use Password Manager. The auto-fill feature will stop working, as well as the ability to generate passwords.

At the end of the 90-day grace period, you have 30 extra days to contact Bitdefender support and request to restore your passwords back to the live database. You will then be able to export your passwords from Bitdefender Password Manager.

Your data will be kept in the live database only until the end of the day it was restored on demand. At midnight the database is erased – and if you have not yet exceeded the 30-day extra period, passwords can be restored again from backup. Raw database data from the backup can be provided upon request to the user, but the database is encrypted and the information cannot be accessed.

What is a Master Password, and why do I have to remember it?
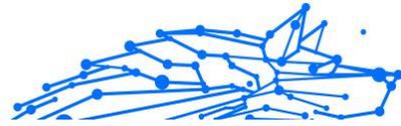
The Master Password is the key that unlocks the door to all the passwords stored in your Bitdefender Password Manager account. The master password must be at least 8 characters long. So create a strong master password, memorize it, and never share it with anyone. To create a strong master password, we recommend you use a combination of uppercase and lowercase letters, numbers, and special characters (like #, $, or @).

How can I stop Bitdefender from asking for my Master Password every time I open the browser?

If you lock your device without closing your browser, Password Manager doesn't lock and you can access your data when you return. As a security measure, every time you open the browser you have to sign in with your Bitdefender Central account and then input your Master password.

❍ To stop the Central sign-in prompt, go into ⬚ Settings and tick "Disable login tab on startup".

❍ To stop the master password prompt, check the "Remember me" box on the Unlock your vault screen.

Why don't you store my Master Password, and what happens if I forget it?

The reason why we don't store your Master Password on our servers is so that only you can access your account. It's the most secure way. If Bitdefender Password Manager doesn't recognize your master password, make sure you type it correctly and the Caps Lock key is not active on the keyboard.

If you forget the master password, you can always use the Recovery Key to unlock Password Manager. During the sign-up process, Bitdefender Password Manager provides a **recovery key** that can be used to regain access to the account without losing your data.

If you forget or misplace both the Master Password and the Recovery Key, as a last resort, contact a Bitdefender representative to reset your account.

> ⚠️ Important
> Resetting your account will erase all your data and passwords saved in Bitdefender Password Manager.

Can multiple users share one Bitdefender Password Manager subscription?

For now, the ability to have multiple users on the same Password Manager subscription is not available but we are working on enabling this feature in the near future.

What is Offline mode and how does it work?

Offline mode is automatically activated when the Internet connection drops while using Bitdefender Password Manager. If you are already signed in and have entered your master password, Offline mode lets you access your passwords when an Internet connection is out of reach.

How do I uninstall Bitdefender Password Manager?

To uninstall Bitdefender Password Manager:

❍ On Windows and macOS:
Remove the Password Manager extension from your web browser. Right-click on the Bitdefender icon and select "Remove".

❍ On Android:
Tap and hold the Password Manager app, then drag it to the top of the screen where it says "Uninstall".

❍ On iOS & iPadOS:
Tap and hold the Password Manager app until all apps on your screen begin wiggling, then tap the X to the top left of the Bitdefender icon.

Privacy & Security questions about Bitdefender Password Manager

Could Bitdefender employees see my passwords?

Absolutely not. Your privacy is our top priority. This is the main reason why we do not store your master password on our data servers: so that no one has access to your account, not even company employees. Every password and account are highly encrypted with the strongest data security algorithm, and the code we see simply looks like a random string of numbers and letters jumbled together.

What would happen if Password Manager servers were hacked?

Each password is encrypted locally on your device before it gets anywhere near our servers, so if hackers were to break into our system, they would only get pages of random letters and numbers without your key to decrypt

them. This means that you and your account details are always safe with us.

7. GETTING HELP

7.1. 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.

7.2. 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.

7.2.1. 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/.

7.2.2. 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/

7.2.3. 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/.

7.3. 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/

7.3.1. 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.