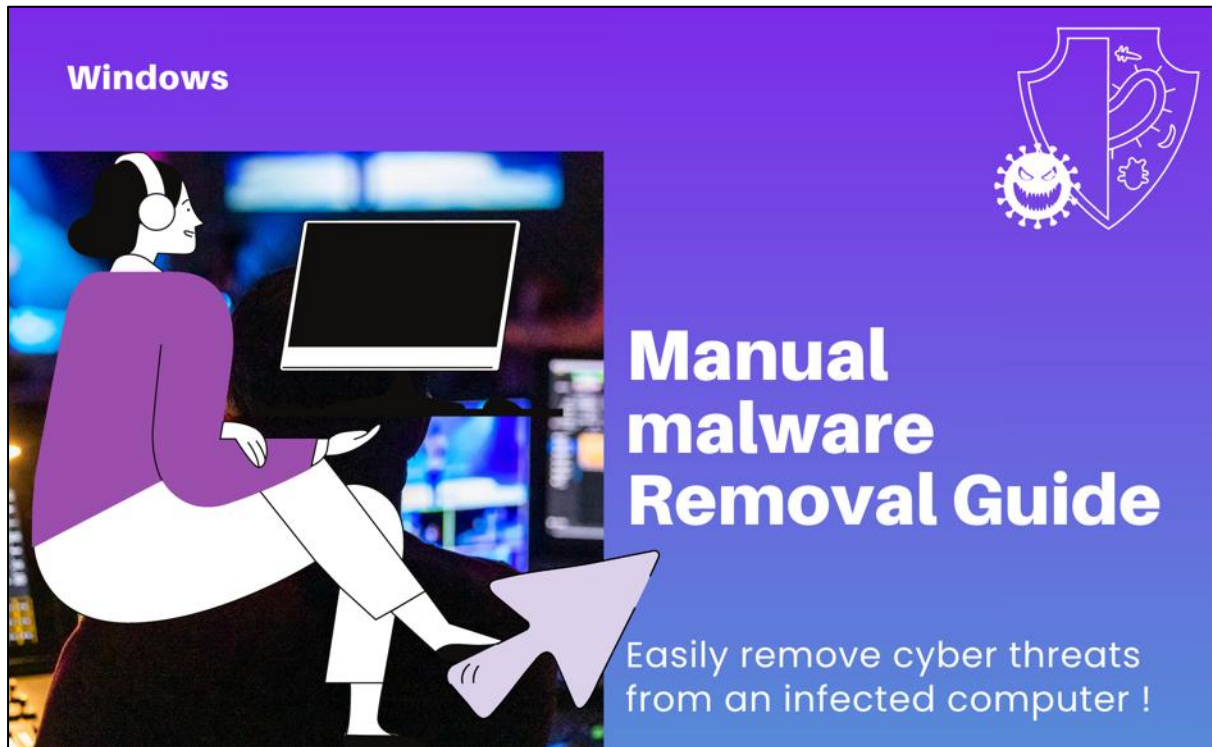


How to manually Remove Malware & Infected files from a Windows computer

This article contains resources to help you manually remove malware and any infected file from your Windows-based computer.



Manual malware removal guide

To manually remove an infected file from your computer, you need to perform the steps below. We recommend manually deleting an infected file only if you are sure the file isn't an important operating system file. Deleting a system file may result in the malfunction of your operating system. Check out the list below to find out which common files can be deleted without hesitation. If you are not sure about the file, please contact Bitdefender Support.

1. Restart the computer in **Safe Mode**. You can do that, by following the steps in our article, [here](#).
2. Display hidden objects in Windows. Information on how to display the hidden object can be found [here](#).
3. Locate and delete the infected file: right-click on the file and then select **Delete** in the menu.
4. After you do this, you can restart the computer normally and run a Bitdefender System Scan to be sure the computer is clean.

Note: If Bitdefender still detects infected files that cannot be resolved, run a System scan and send the log to our Support Team via the open ticket you have with us. Check out this article to learn [How to Scan a PC for viruses with Bitdefender & Export the scan Log](#). If you don't have a ticket, please use the contact form.

Common file types that can be safely deleted

Temporary Windows Files

The Temporary files are usually recognized as follows:

- .tmp files found on **C:**, **C:\Windows**, **C:\Windows\temp**, etc.
- files found in these folders: **C:\Windows\Temp**, **C:\Users\AppData\Local\Temp**

For more details and step-by-step instructions, please check this article – [How to clean infected Temporary Files](#).

① Note

In the example above, **C:** represents your default system drive. The system drive is the primary hard drive in your computer that stores the operating system and primary boot volume. If you don't have Windows installed on the C partition, please modify the paths accordingly.

Temporary Internet Files

A temporary internet file is a file used by browsers to store data for every web page or URL address that you visit. When the server sends the web page files to the browser, they are stored in a file so that the next time you visit the site, the browser takes the data from the temporary Internet file.

The Temporary Internet Files can be found in different locations depending on the internet browser:

- For Mozilla Firefox: Type **about: cache** in the address bar. The upcoming page reveals the cache folder.
- For Google Chrome: **C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Default\Cache**
- For Internet Explorer: [follow these steps to delete cached images and temporary Internet files](#).

To learn more about deleting temporary Internet files, check out [this article](#).

Files located in System Volume Information

Check [this](#) KB article to learn how to clean system restore points from **System Volume Information**.

Email archives that cannot be repacked by Bitdefender

For more details and how to clean an infected email, please check [this](#) article.

For files located on optical devices such as CDs, DVDs, Blu-ray Discs

Unfortunately, these files cannot be cleaned since modify/delete actions are not permitted on this kind of storage devices. You can rest assured that if you still want to use the respective device, Bitdefender on-access scanning will protect your PC from any attack. However, we recommend you take safety measures or not using at all computers without an up-to-date security solution.

Files located on network storage, NAS, network shares, mapped network drives, etc.

There are several reasons for Bitdefender not being able to clean the respective files, such as:

- You only have read permissions on the respective network share/storage; therefore, no actions can be taken due to limited privileges
- The network share has a different operating system, not supported by your Bitdefender virus engines.

You can rest assured that, if you still want to access this share, Bitdefender On-Access Scanning will protect your PC from any attack.

Tmp.ebd files

To remove the infected Tmp.ebd file from your computer, you need to reset the **Windows Update** and **Windows Search** services by following these steps:

1. Temporarily disable **Bitdefender Antivirus** from **Protection > Antivirus > Open > Advanced > Bitdefender Shield**.
2. Type **services.msc** in the Windows Start menu and hit **Enter**.
3. Locate the **Windows Update** service, right-click on the entry, and choose **Restart** from the dropdown menu.
4. Locate the **Windows Search** service and restart it as well.
5. Reboot the PC and check if the issue reoccurs.