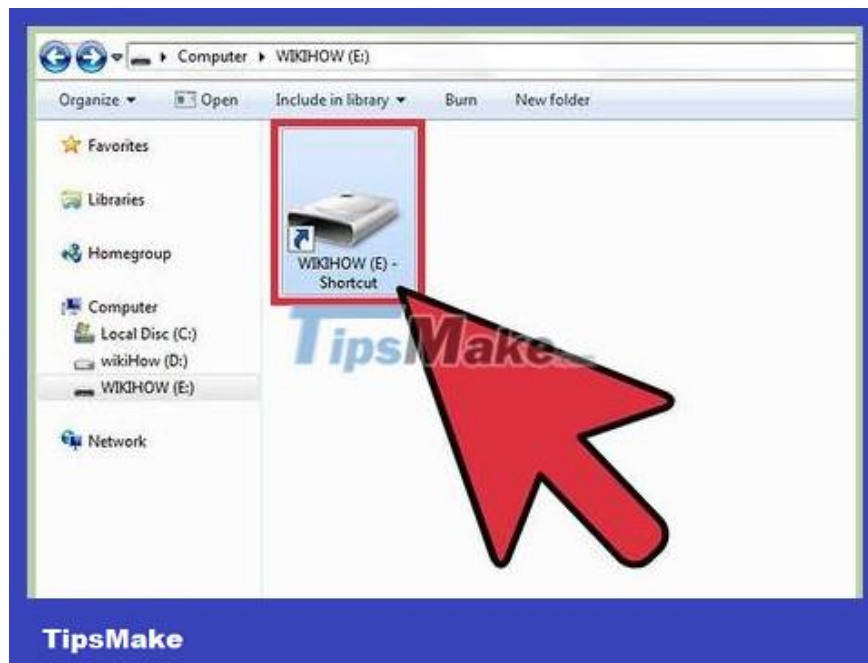


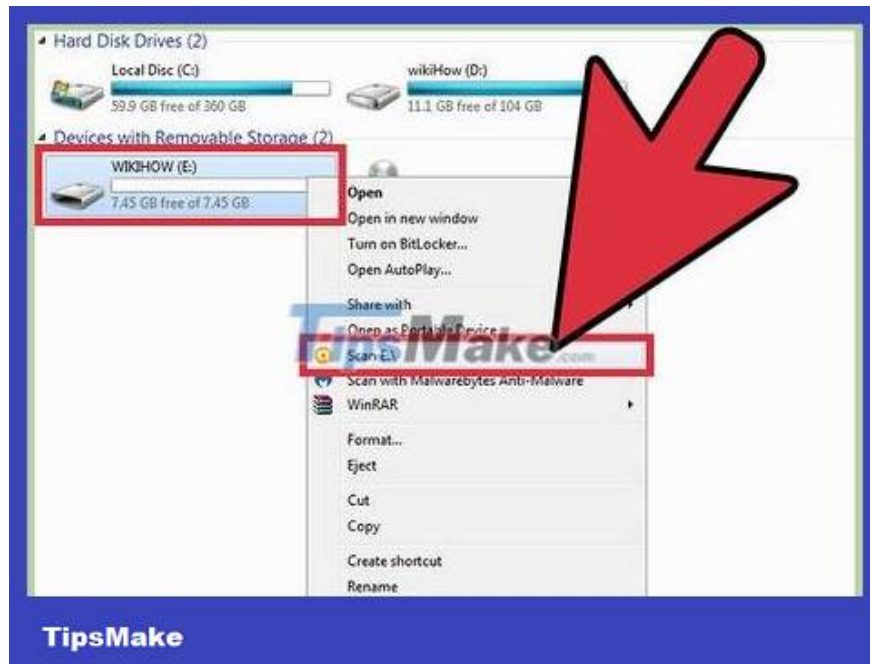
# How to Remove Viruses from Flash Drive

Because of their portability, USB devices are easy means of spreading viruses. USB devices are vulnerable to two main types of viruses: shortcut creation viruses and autorun viruses. In this article, we will discuss how to remove viruses using an anti-malware program or entering the command yourself. Learn about the measures Windows is taking to protect your computer from autorun viruses.

## Kill viruses and create shortcuts



**Learn about viruses that create shortcuts.** Viruses that create shortcuts come in two forms. Type 1 is a virus that replaces folder and file icons on your computer with shortcut icons—icons with an arrow in the lower left corner, and the word 'shortcut' in the name, and/or an extension. 'shortcut.exe'. Type 2 is a virus that affects USB or pen drives (portable hard drives). This type of virus will put all files on the USB into a hidden folder and create a shortcut.exe file of the pen drive. When you open these files, you will activate viruses and they will spread to your computer.

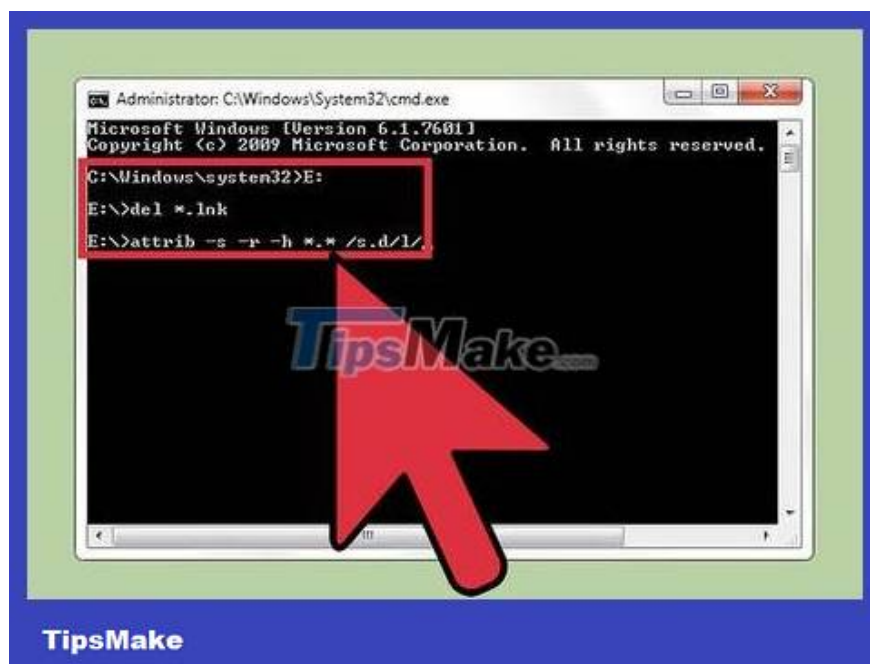


**Delete viruses that create shortcuts with anti-virus software.** If your USB is infected with a shortcut virus, you can remove the malicious error with antivirus software. Select Start > My Computer. Right-click on the removable drive and select 'Scan for Viruses'. Follow the on-screen instructions to remove the shortcut virus.

If you are using Windows RT 8.1 or later, your computer will be equipped with Windows Defender. You can use this program to scan for viruses. Start Windows Defender and select Settings > Advanced. Check the 'Scan removable drives' dialog box. Each time a comprehensive scan is performed, the USB will be checked for viruses.

If your computer is not equipped with anti-virus software, download a reputable anti-malware program.

You should only download and install an anti-malware program.



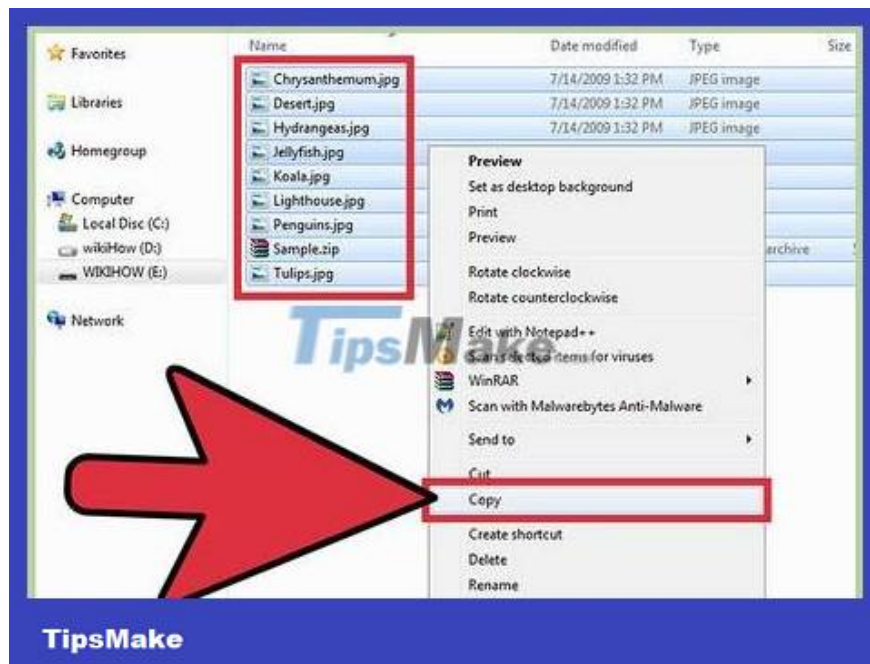
**Remove shortcut virus with command prompt.** You can remove viruses from flash drives (removable drives) using a command prompt window. To open a command prompt window, click 'Start' and type 'cmd'. Click 'cmd' or 'Command Prompt Window' in the list of results and select 'Run as Administrator'. In the command prompt window:

Enter the letters USB and press ? Enter. To identify the letter corresponding to the USB drive, open 'My Computer' and locate the letter written next to the removable drive.

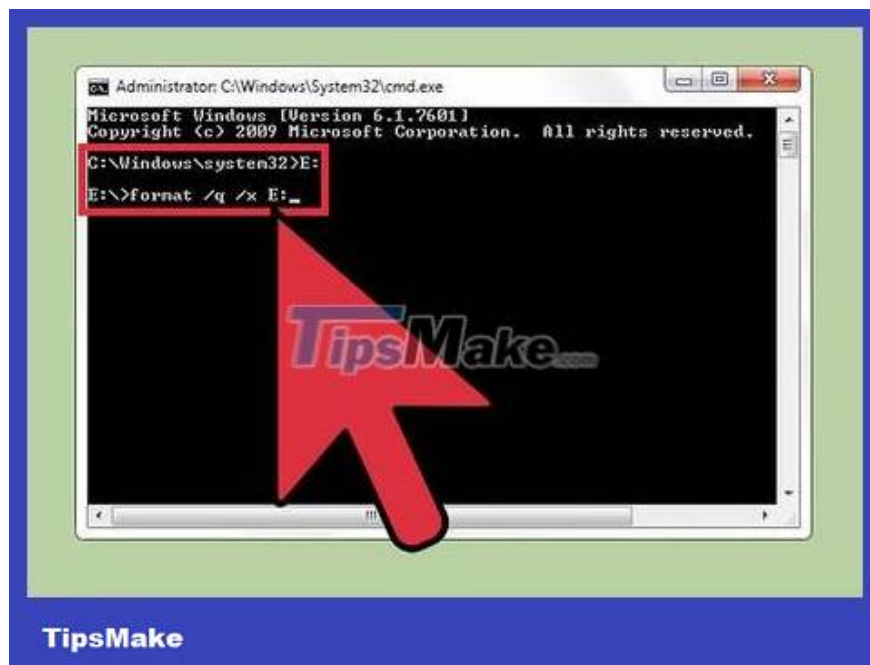
Type **del \*.lnk** and press ? Enter.

Type **attrib -s -r -h \*.\* /sd//** and press ? Enter.

Open the flash drive. All information will return to normal status.



**Backup files.** After removing the virus, you can format the drive. Reformatting the USB will erase all data stored on the drive, helping you clean and remove viruses on the device. Before reformatting, back up all files on USB. Scan the entire directory on the pen drive and delete strange folders and files. Transfer all files from USB to folder on computer.



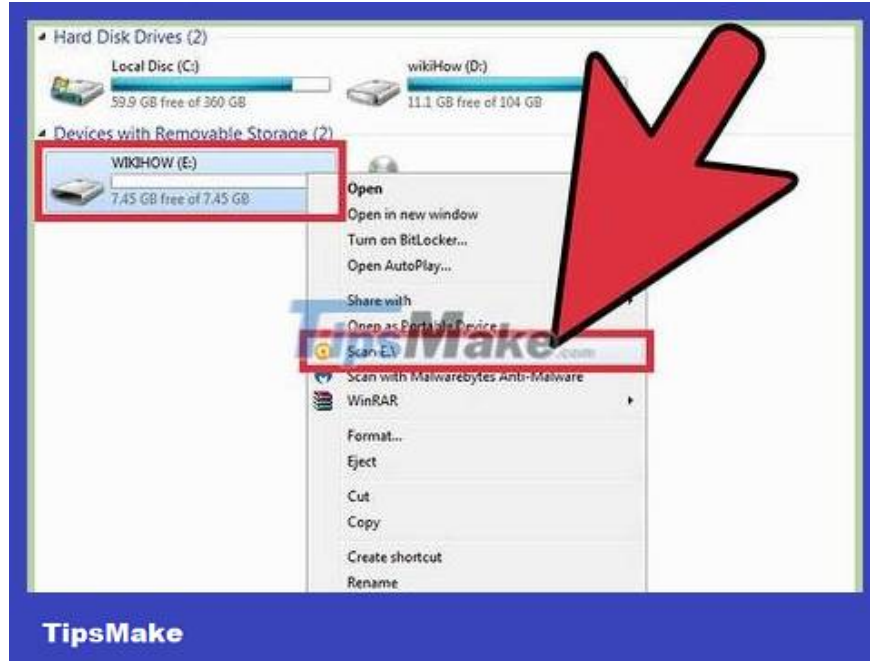
**Reformat the drive.** Click on 'Start' and type 'cmd' in the search bar. Start 'Command Prompt Window'. Type the letter corresponding to the drive and press `Enter`. Type **format /q /x [INSERT DRIVE LETTERS]**; and press `Enter`. Transfer all files back to USB.

### **Kill autorun virus**



**Learn about autorun virus.** Previously, when you plugged a USB into a port on your computer, the drive would automatically open. If your USB is infected with a virus, this process will execute the **autorun.inf** file containing the autorun virus. Thus, when the USB drive automatically opens, it will activate the autorun virus. Currently, USB devices do not automatically open on Windows XP, Windows 7, Windows 8 and Windows 10, meaning the **autorun.inf** file will not automatically execute. This solution will protect your computer from

viruses.

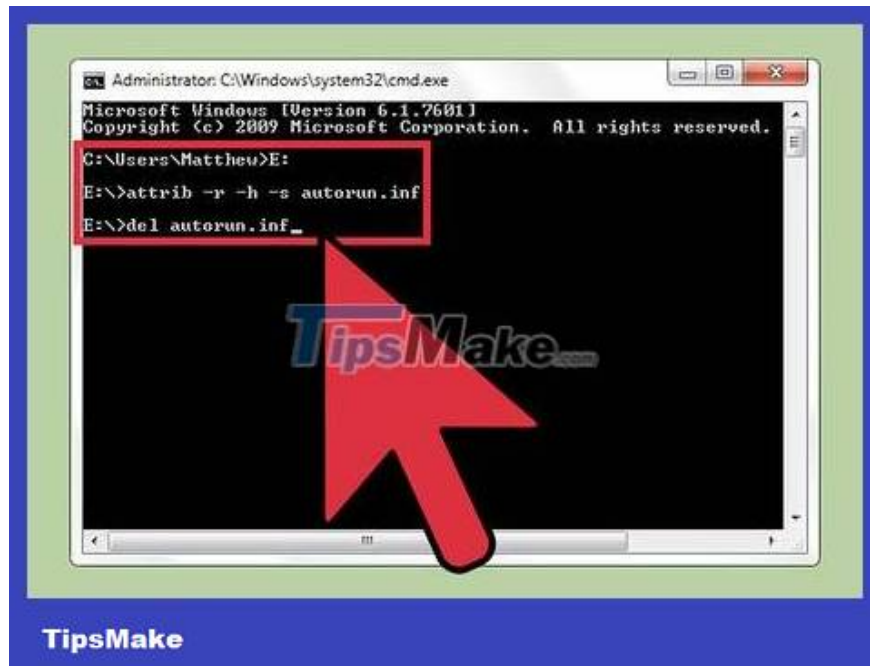


**Scan for viruses on the drive.** You should scan the pen drive for viruses before using it. Click Start > My Computer. Right click on the removable drive and select 'Scan for Viruses'. If a virus is detected, follow the instructions to remove it.

If you use Windows RT 8.1 or later, your computer is equipped with Windows Defender. To scan for viruses, open Windows Defender. Click Settings > Advanced. Check the 'Scan removable drives' dialog box. Each time a comprehensive scan is performed, the USB is also checked for viruses.

Some anti-malware programs will automatically scan your USB when you insert it into a port on your computer.

If your Windows computer is not equipped with an anti-virus program, download and install a reputable program.



**Kill autorun virus.** To remove viruses from removable drives, you need to delete the autorun.inf file and restart the computer.

Click Start > Run.

Type 'cmd' and press ? Enter.

In the Command Prompt Window, type the letter corresponding to the drive and press ? Enter.

Type **attrib -r -h -s autorun.inf** and press ? Enter.

Type **del autorun.inf** and press ? Enter.

Restart the computer after completion.

Haris Shafi.

You finished reading the article "**How to Remove Viruses from Flash Drive**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.