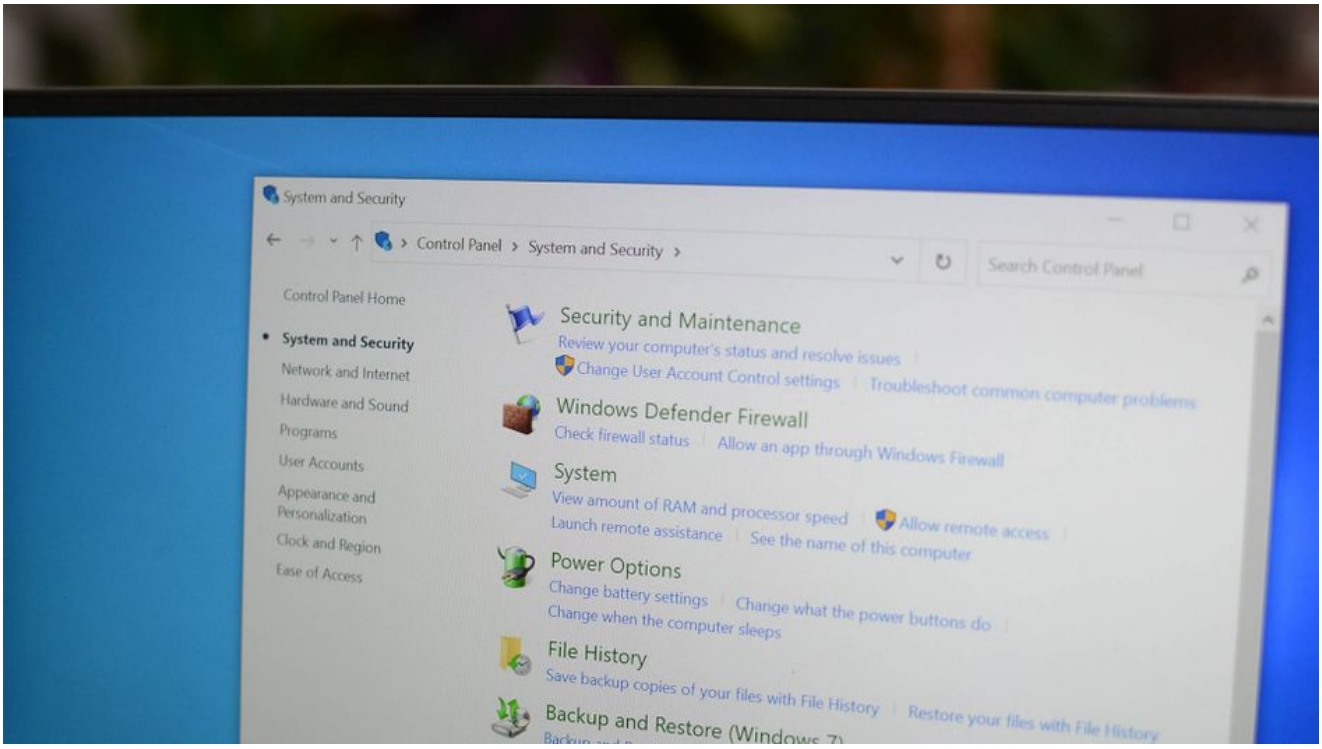
Suspect Your Windows PC Has Malware? How to Quickly Reduce and Remove the Threat

howtogeek.com/reduce-windows-malware-threat

December 25, 2023

- Home
- Windows

By Efam Harris
Published Dec 25, 2023
If you think your Windows 10 or 11 computer has been compromised, here are the steps you should take immediately to minimize the impact.



Jason Fitzpatrick / How-To Geek

If you suspect your PC is infected with malware, or you get a legitimate warning from a tool like Microsoft Defender telling you as such, there are steps you should take immediately to minimize the impact and cure your computer. Whether you're running Windows 10 or 11, here's what you need to do.

Turn Off Your Internet and Disconnect Devices

The first thing you should do is disconnect your internet and any local connections. This does not remove the malware, but it prevents the attacker from accessing your PC, and stops them using your system to attack other computers within your network.

Disconnecting your internet is important to reduce the malware's impact, but it doesn't remove the threat entirely because malware can work offline to delete and modify files and applications.

If you have a wired connection, the quickest thing to do is simply pull the Ethernet cable out of your system.

If you use a wireless network, press Win+i to open Settings. Select "Network and Internet" to open the network settings.

Click "Wi-Fi," then "Show available networks." Choose your active connection, then click "Disconnect."

Next, disconnect all non-essential devices connected to your computer, since the malware may attempt to access them. If you do not need it to operate the computer, like an external hard drive, then you should disconnect it. This even includes devices like a mouse—if you're on a laptop and can use the trackpad instead, do so.

Run a Quick Malware Scan Using Microsoft Defender

Next, you need to run a scan to confirm if there’s malware on your system. Every Windows 10 and 11 computer comes with Windows Security, which includes an antivirus tool called Microsoft Defender. You can run a quick Microsoft Defender scan to find potential threats and quarantine them.

To begin a scan, open Start, type "Windows Security", and click to open.

Next, select "Virus & Threat Protection."

Then click "Quick Scan" to initiate a scan.

Your scan should start immediately. It will show you the progress, like estimated time remaining and number of files scanned.

Once the scan is complete, it tells you whether any threats were discovered.

Quick scans run surface-level checks for potential threats, and are great for verifying and removing malware quickly, unlike the full scan option which can take hours. However, by design it's not as comprehensive as a full scan—that's where the Microsoft Safety Scanner comes in.

Run an Extensive Malware Scan Using Microsoft Safety Scanner

While Microsoft Defender is a good initial malware scan, you should next run an extensive scan with Microsoft Safety Scanner. This doesn't come with your computer, so download the 32-bit or 64-bit version directly from Microsoft.

Microsoft Safety Scanner only runs when manually activated. The Safety Scanner is valid for 10 days after download. To rerun a scan with updated anti-malware definitions, download the Safety Scanner again.

Once downloaded, open the "MSERT.exe" file to launch the Microsoft Security Scanner.

Click "Run" in the security warning pop-up to approve.

Accept the terms of the license agreement and click "Next" to proceed.

On the welcome page, click "Next" to advance.

Select the "Full Scan" option and click "Next" to begin the scan.

The scan can take several hours to complete. In the meantime, you should proceed with the other steps in this article, and return when the scan is complete.

At the end of the scan, Windows removes the malware for you. To finish, click "Restart" to restart your PC. You can also view the results of the scan by clicking "View detailed results of the scan."

Terminate Suspicious Applications in Task Manager

While the scan runs, use Task Manager to terminate suspicious applications. To begin, press Ctrl+Alt+Del and click "Task Manager." If you're not on it by default, go to the "Processes" tab.

Scroll the list of processes to see if you can identify any unusual, suspicious, or unauthorized applications or background processes. These come in different formats, so spotting them might be difficult, but if you're unsure about anything, right-click it and select "Search Online." A web page with more information opens. If it's a known malware or harmful process, you'll know from the documentation.

If you find an unauthorized application that’s running, right-click that application and then click "End Task." This stops the process from running in the background.

If you don’t find any unauthorized processes, are unsure what tasks you should end, or find that they reopen once you've ended them, don’t worry; the full scan should take care of it. In the meantime, you can check for suspicious user profiles.

Remove Unknown Users in Computer Management

Malware may create unauthorized user accounts on your PC, so you should check and remove them. To do this, use the Computer Management tool.

To begin, open the Start menu, search "Computer Management", and click to launch.

In the left panel, double-click "Local Users and Group," then double-click "Users." A list of users appears in the main panel.

Ensure you are familiar with every username. If you find an unidentifiable user, right-click the user and "Delete" it.

Wipe Your PC and Reinstall Windows

After all that, if you still experience signs of a potential virus, such as missing files, frequent crashes, and a very slow computer, you may need to wipe your PC clean and reinstall Windows afresh.

Before you wipe your PC, ensure you have a backup from the last time your PC functioned optimally. This must be a clean version before the suspected malware attack; you don’t want to reinstall a compromised backup. Wiping your PC will delete all files, applications and configurations. Your backup should contain all essential documents and files you can’t afford to lose.

A factory reset removes most threats—it's rare for any to survive. For this, you can use the in-built Windows factory reset tool.

To begin the factory reset, press Win+i to open Settings. For quick access, type Reset in the search bar and click "Reset this PC."

This should open the Recovery section. Click "Get Started" (Windows 10) or "Reset PC" (Windows 11) to begin the process. For full information, see our guide to resetting a Windows computer.

Always Practice Strong Cybersecurity Habits

It’s not enough to successfully eliminate malware. You need to prevent it in the first place. Develop good cybersecurity habits, such as using strong passwords, VPNs on public Wi-Fi, and keeping your devices up to date. Many of these habits are basic and do not require high-level technical skills.

Remember, prevention is always better than cure—sometimes there’s no cure, and you could permanently lose sensitive data, money, and devices.