Does Your Computer Have a Virus? Here's How to Check

howtogeek.com/441321/does-your-computer-have-a-virus-heres-how-to-check

Chris
Hoffman

vladwel/Shutterstock.com

Windows computers sometimes do get viruses and other malware, but not every slow or misbehaving PC is infected by malware. Here's how to check if you actually have a virus—and whether that suspicious process is dangerous or not.

What Are the Signs of a Virus?

Poor performance, application crashes, and computer freezes can sometimes be the sign of a virus or another type of malware wreaking havoc. However, that's not always the case: There are many other causes of problems that can slow down your PC.

Likewise, just because your PC is running fine doesn't mean it doesn't have malware. The viruses of a decade ago were often pranks that ran wild and used a lot of system resources. Modern malware is more likely to lurk silently and covertly in the background, trying to evade detection so it can capture your credit card numbers and other personal information. In other words, modern-day malware is often created by criminals just to make money, and well-crafted malware won't cause any noticeable PC problems at all.

Still, sudden poor PC performance may be one sign you have malware. Strange applications on your system may also indicate malware—but, once again, there's no guarantee malware is involved. Some applications pop up a Command Prompt window when they update, so

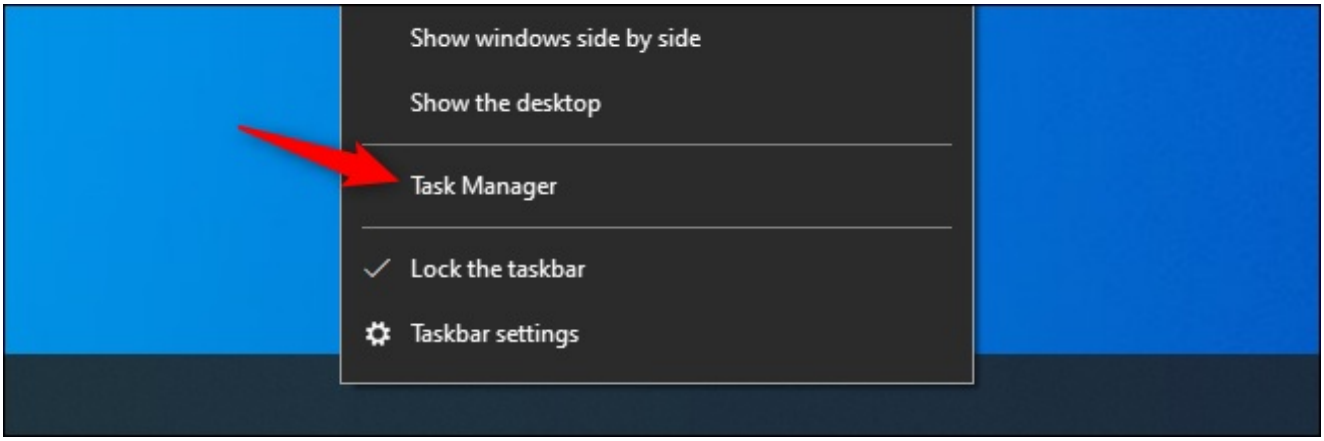
strange windows flashing onto your screen and quickly disappearing may be a normal part of the legitimate software on your system.

There's no one-size-fits-all piece of evidence to look for without actually scanning your PC for malware. Sometimes malware causes PC problems, and sometimes it's well-behaved while sneakily accomplishing its goal in the background. The only way to know for sure whether you have malware is to examine your system for it.

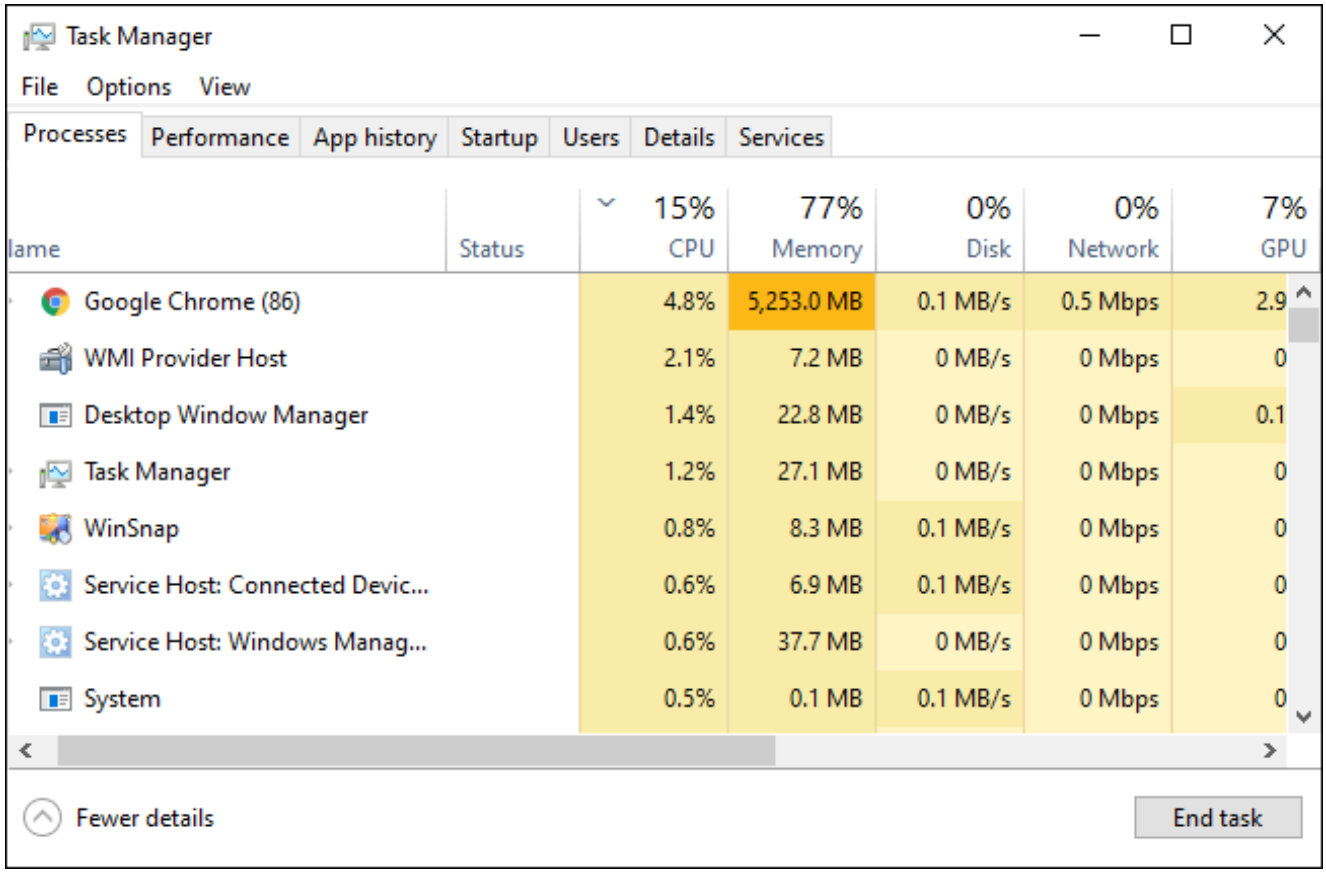
RELATED: ***10 Quick Ways to Speed Up a Slow PC Running Windows 7, 8, or 10***

How to Check if a Process Is a Virus or Not

You might be wondering if your computer has a virus because you've seen a strange process in the Windows Task Manager, which you can open by pressing Ctrl+Shift+Esc or by right-clicking the Windows taskbar and selecting "Task Manager."



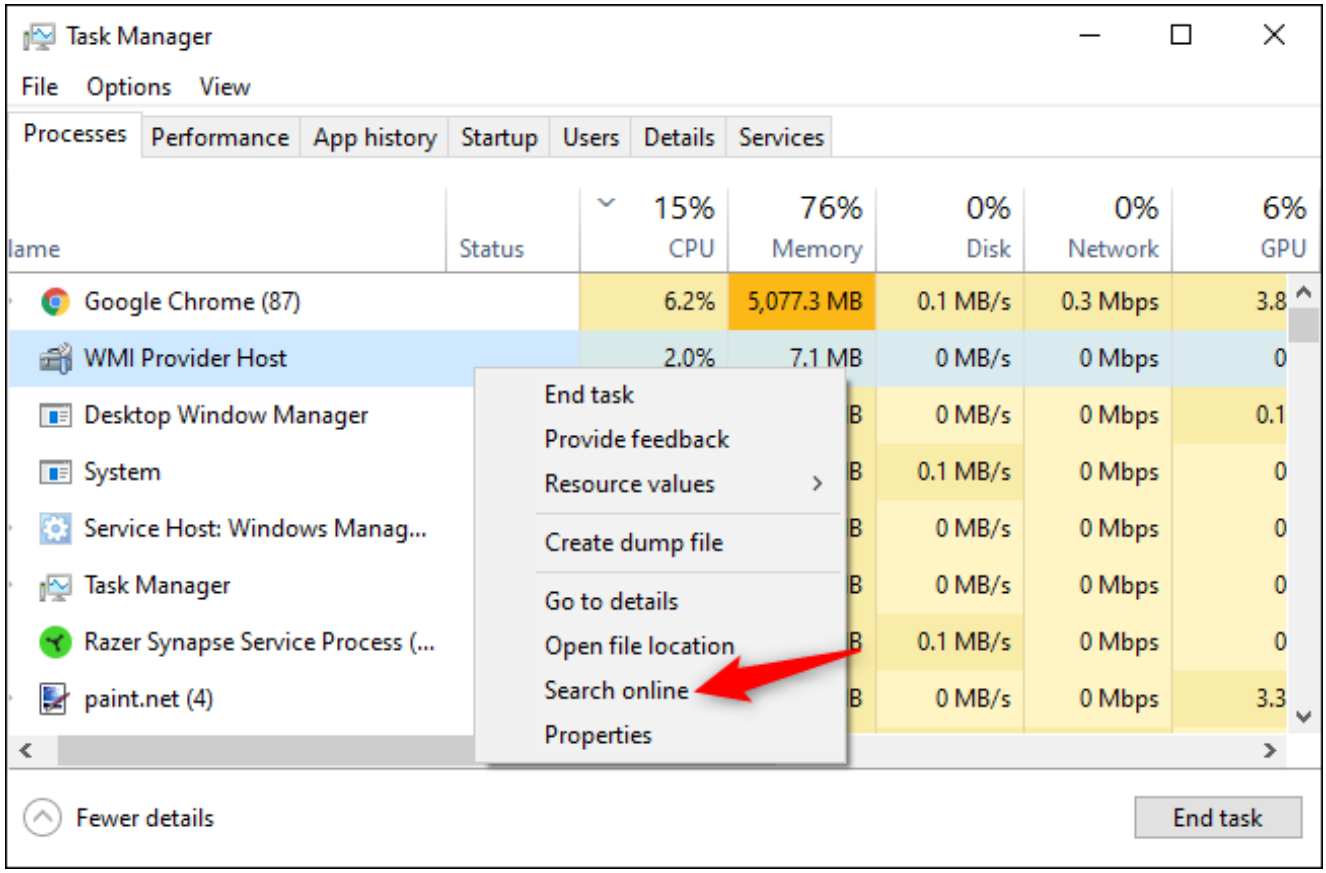
It's normal to see quite a few processes here—click "More Details" if you see a smaller list. Many of these processes have strange, confusing names. That's normal. Windows includes quite a few background processes, your PC manufacturer added some, and applications you install often add them.



Badly behaved malware will often use a large amount of CPU, memory, or disk resources and may stand out here. If you're curious about whether a specific program is malicious, right-click it in the Task Manager and select "Search Online" to find more information.

If information about malware appears when you search the process, that's a sign you likely have malware. However, don't assume that your computer is virus-free just because a process looks legitimate. A process could lie and say it's "Google Chrome" or "chrome.exe," but it may just be malware impersonating Google Chrome that's located in a different folder on your system. If you're concerned you might have malware, we recommend performing an anti-malware scan.

The Search Online option isn't available on Windows 7. If you use Windows 7, you'll have to plug the name of the process into Google or another search engine instead.

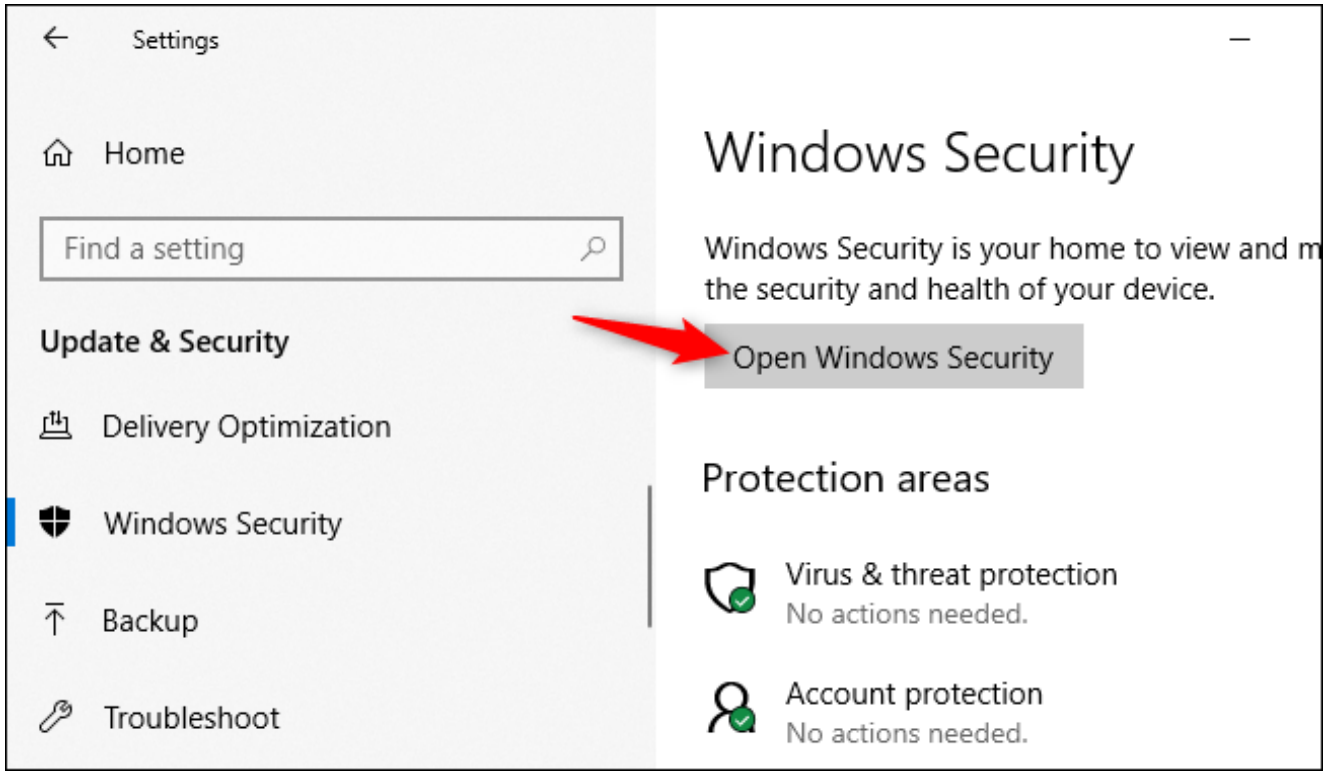


RELATED: ***What's the Best Antivirus for Windows 10? (Is Windows Defender Good Enough?)***

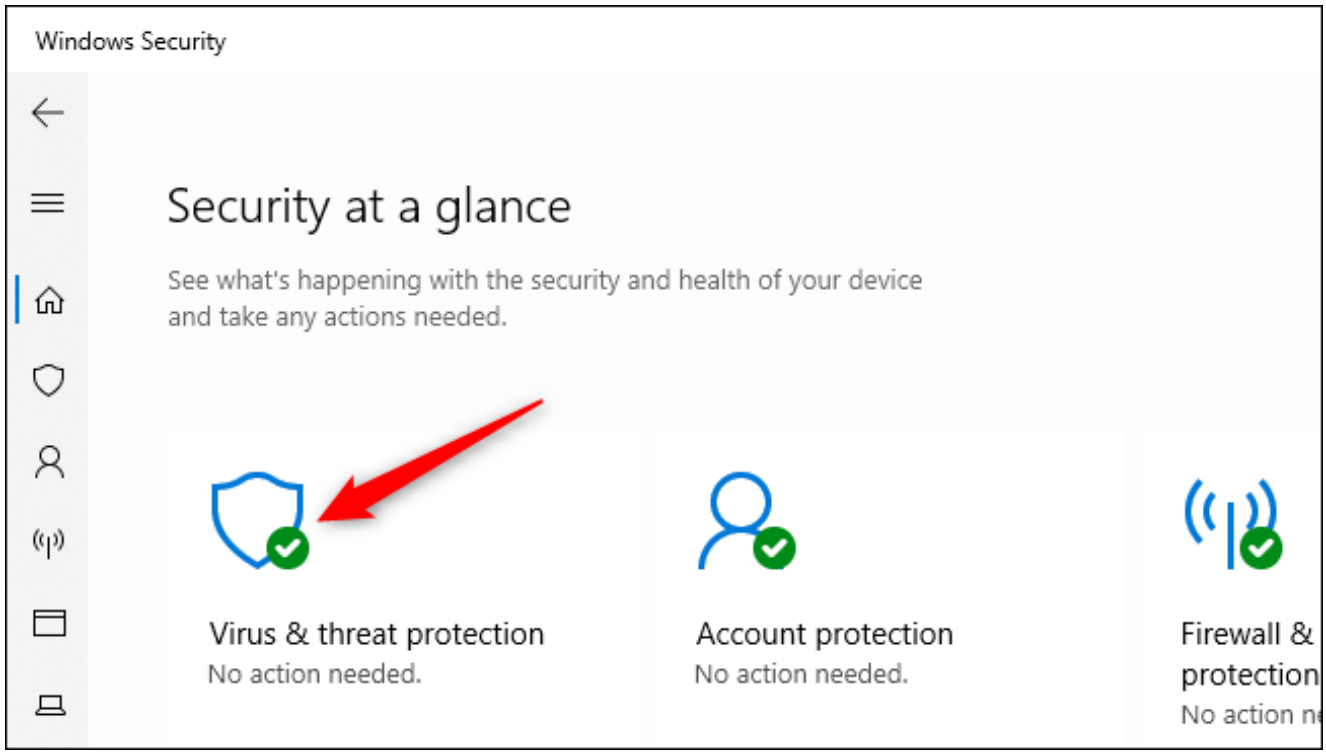
How to Scan Your Computer for Viruses

By default, Windows 10 is always scanning your PC for malware with the integrated Windows Security application, also known as Windows Defender. You can, however, perform manual scans.

On Windows 10, open your Start menu, type "Security," and click the "Windows Security" shortcut to open it. You can also head to Settings > Update & Security > Windows Security > Open Windows Security.



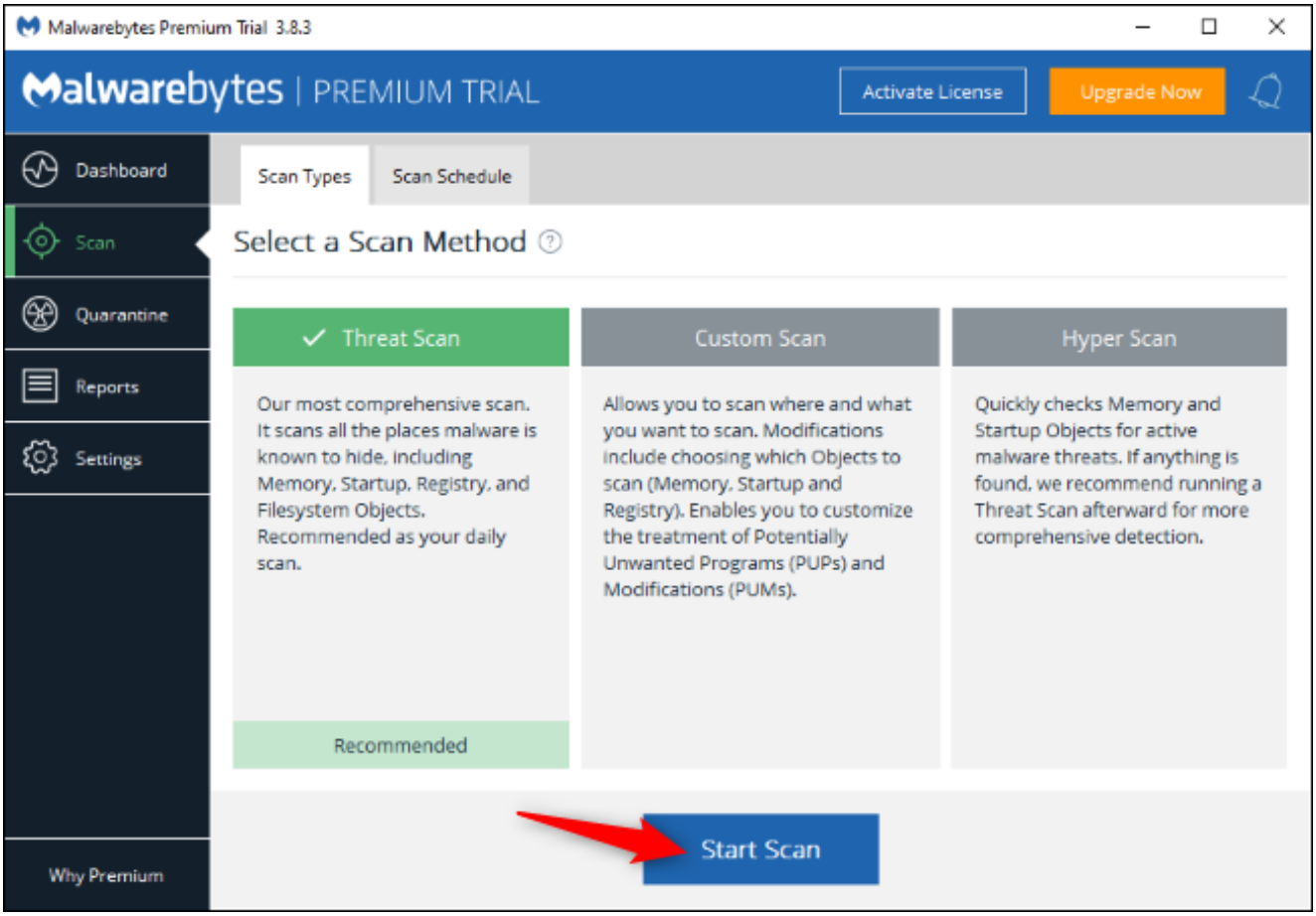
To perform an anti-malware scan, click “Virus & threat protection.”



Click “Quick Scan” to scan your system for malware. Windows Security will perform a scan and give you the results. If any malware is found, it will offer to remove it from your PC automatically.

If you want a second opinion—always a good idea if you're concerned you might have malware, and your primary antivirus doesn't find anything—you can perform a scan with a different security application, too.

We like and recommend Malwarebytes, which pairs well with Windows Security to provide an extra layer of protection for your PC. The free version of Malwarebytes will let you perform manual scans to check for viruses and other malware on your PC. The paid version adds real-time protection—but, if you're just looking to test a computer for malware, the free version will work perfectly.



Windows 7 doesn't include built-in antivirus software. For free antivirus, you can download Microsoft Security Essentials and run a scan with it. This provides similar protection to the Windows Defender security software built into Windows 10.

If your antivirus application finds malware but has trouble removing it, try performing a scan in Safe Mode. You can also ensure you don't have malware on your PC by resetting Windows 10 to its default state.

RELATED: ***How to Remove Viruses and Malware on Your Windows PC***

READ NEXT