6 ways to check if a downloaded file is safe before using it.

Better safe than sorry, which is why you should always check that your downloaded files are safe before opening them.

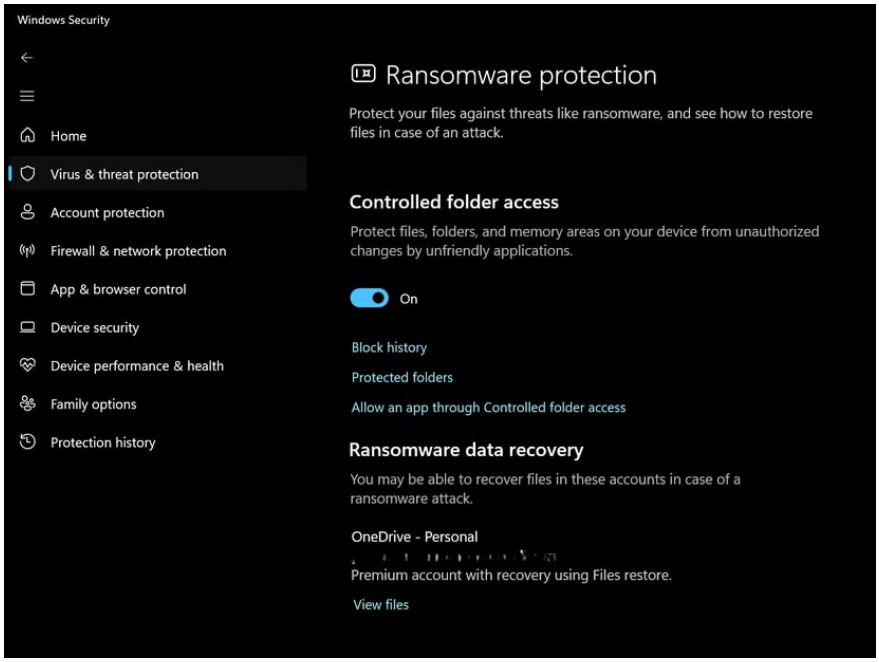
Downloading files from the internet is dangerous because malware , trojans , and ransomware can disguise themselves as harmless downloads. However, better safe than sorry, which is why you should always check that your downloaded files are safe before opening them.

1. Free online virus scanning tools

6. Use Windows Security (or built-in antivirus software)

The easiest way to check downloaded items is to use Windows Security , which is pre-installed on your PC. Windows Security (formerly known as Windows Defender) runs in the background but can scan for suspicious files you download.

To scan a file, right-click on it and select **Scan with Windows Security** from the menu. The scan usually only takes a few seconds and provides immediate peace of mind. For maximum protection, make sure you also have Ransomware Protection enabled in your Windows Security settings.



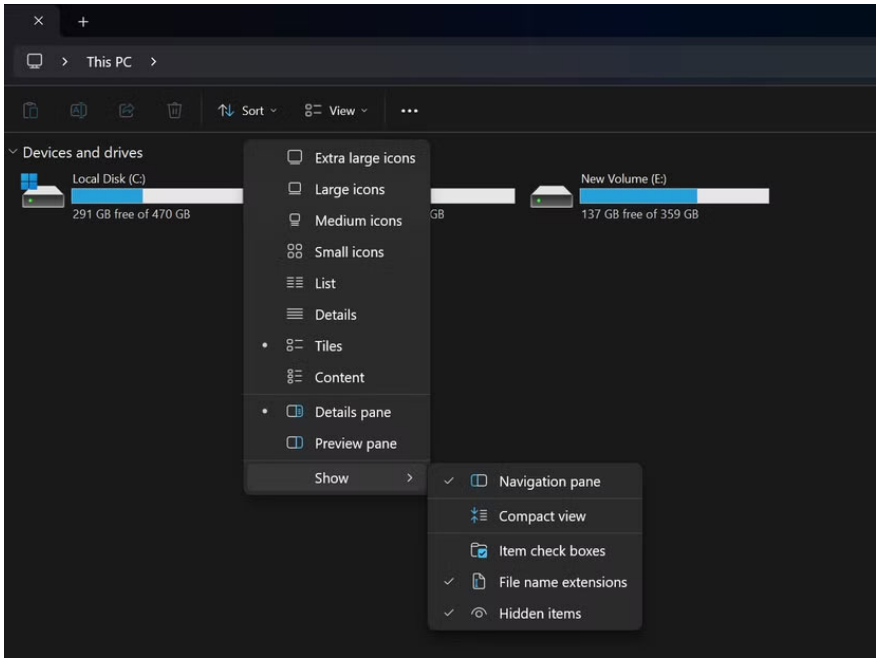
But what about those attractive paid antivirus programs? Frankly, Windows Security has improved significantly over the years. Unless you handle extremely sensitive data or frequently access the dark corners of the internet , the built-in protection will effectively handle most threats. This is especially effective when combined with the essential Windows 11 security checklist.

Mac and Linux have similar built-in protection features, although they operate differently. Regardless of your operating system, always scan downloaded files before opening them, especially executable (.exe) files or script files that could potentially run malicious code on your system.

5. Verify the file extension before opening it.

One of the oldest tricks in the cybercrime handbook is disguising malicious files with fake extensions. That harmless-looking "photo.jpg" could be "photo.jpg.exe" waiting to wreak havoc on your computer.

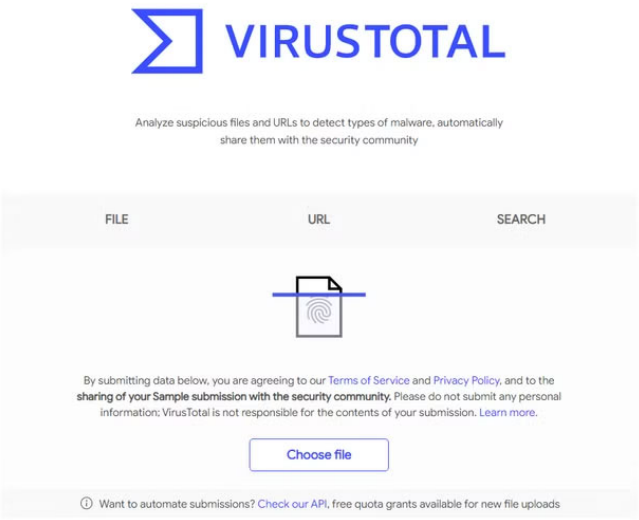
By default, Windows hides file extensions , which is entirely within the reach of hackers. However, you can adjust Windows settings to see each file extension individually . This simple change provides you with the necessary layer of protection against disguised malware.



You should be wary of executable files (.exe , .bat , .cmd, .vbs, .js, .wsf, and .scr) from unknown sources. These file types can run code on your computer without much restriction. Therefore, detect and avoid these malicious EXE files to prevent problems. Furthermore, documents containing macros (.docm, .xlsm) may also contain malicious code.

Note : Pay particular attention to double extensions like "invoice.pdf.exe" or "movie.mp4.scr" which attempt to conceal their true nature. The second extension will reveal what the file actually is, regardless of the icon displayed.

4. Use an online virus scanning service.



If you're still unsure about a file, seek a second opinion. Online virus scanning tools like VirusTotal will analyze your suspicious files using dozens of antivirus tools simultaneously, which is more convenient than relying on a single scanner.

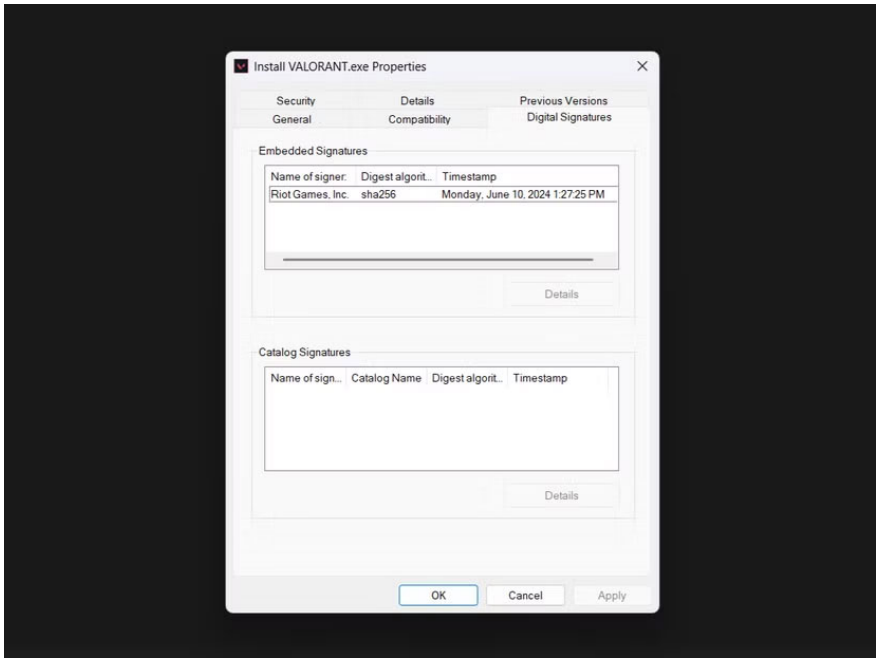
Using VirusTotal and similar tools is simple: Upload the suspicious file to the website and wait for the results. VirusTotal tells you how many of their more than 70 security tools flagged your file as suspicious. This collective approach significantly reduces the chances of malware slipping through undetected.

These online scanners are very handy because they work regardless of your operating system. They're quite useful for unusual file types that your antivirus software might not be optimized to detect. Just remember that files you upload to these services are usually stored on their servers, so avoid sending sensitive personal documents.

1. Safe websites for downloading free software

3. Verify the digital signature and hash file.

Legitimate software companies digitally sign files to verify their authenticity. If a file's digital signature is missing or displays an unknown publisher, that's a sign worth investigating. Fortunately, we can check file digital signatures in Windows. To do this, right-click on any downloaded program, select **Properties** , and then check the **Digital Signatures** tab .

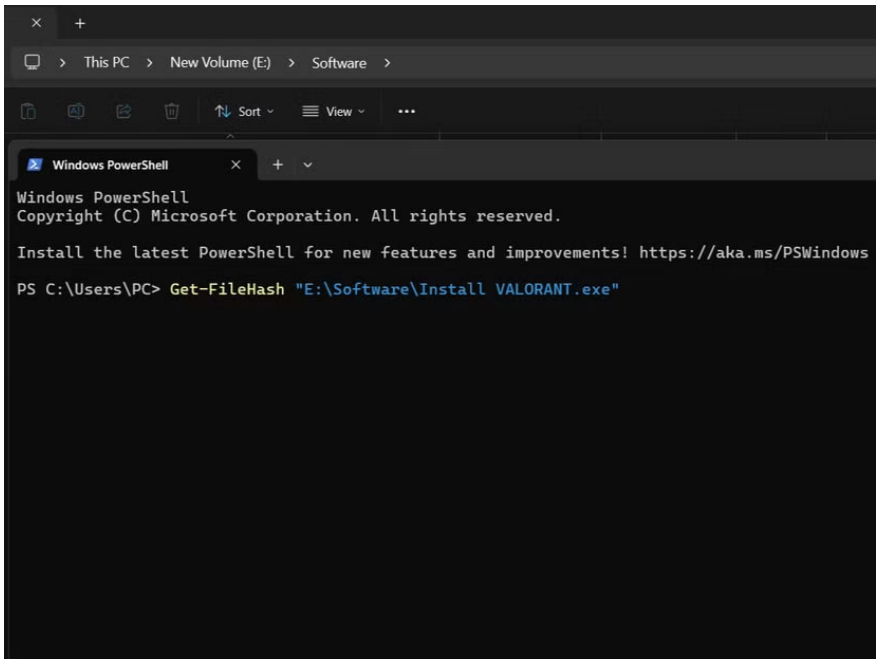


File hashes are also a useful security check. They act as a unique identifier for files, similar to DNA. Developers often publish hash values ??along with download links when downloading software from official sources. By comparing the published hash value with the hash value of the downloaded file, you can verify that nothing has changed during the download process.

Creating a hash file in Windows is easier than you think.

1. Type **Windows PowerShell** into the Start menu search bar and open **Best Match** .

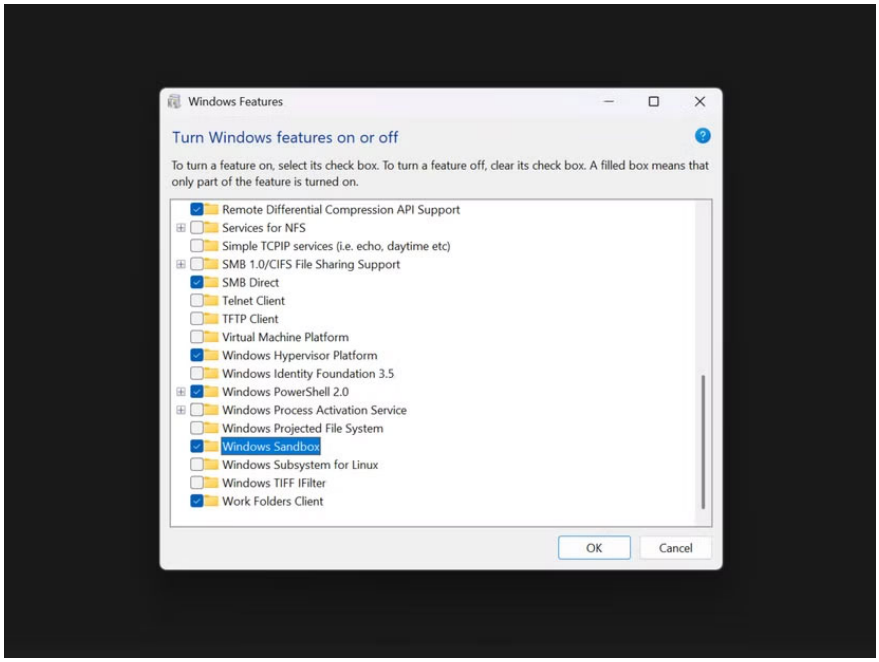
2. In PowerShell , type **Get-FileHash** , press the spacebar, followed by the file path, and press **Enter** . You can copy the file path from the address bar of Windows File Explorer.



Compare this output to the developer's published hash—they must match exactly. This verification step is crucial for software updates and security tools, where even minor modifications can indicate tampering.

2. Run the suspicious file in a sandbox environment.

Sometimes, you come across files that seem suspicious, but you still need to open them. Instead of risking your main system, consider running them in a sandbox, a lightweight desktop environment designed to test suspicious software. If the file is malicious, the damage will be limited to the sandbox.



If you have Windows 10 or 11 Pro, you can directly access Windows Sandbox. It only takes a few minutes to enable and set up Windows Sandbox, providing an instant safety net to check for suspicious downloads.

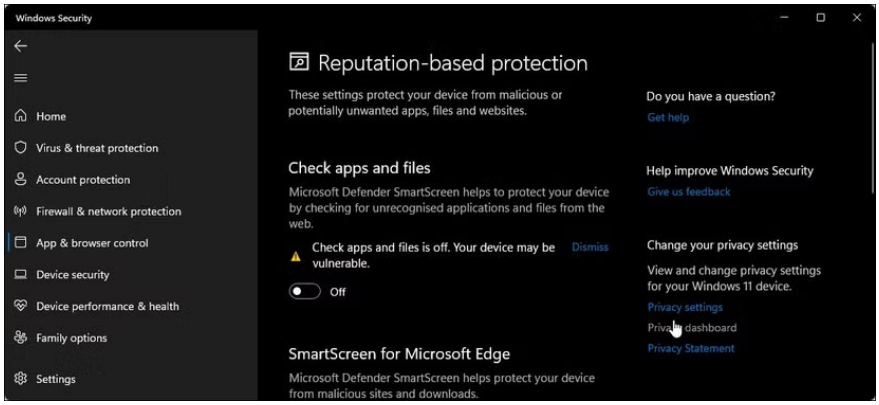
Don't have Windows Pro? No problem, you can use free online sandbox tools, like ANY.RUN and Hybrid Analysis. They allow you to upload files and watch them execute in a safe environment. Some can even generate reports showing exactly what the file attempted to do – network access, registry key modification, hidden file creation, etc.

After the scan, the entire environment will disappear, taking with it any potential malware. If you frequently check unknown files, consider setting up a dedicated virtual machine that you can easily reset after each use.

1. Do not turn off security alerts or SmartScreen.

We've all been in this situation: You're in a hurry to install something and those annoying security warnings keep popping up: "Windows has protected your PC," "This file may be dangerous." You might want to click **Run anyway** or permanently disable these protections, especially when you're sure the file is safe.

However, these security alerts exist for a good reason, as Windows SmartScreen and similar protection features help keep systems safe from viruses. In fact, they often detect malware that traditional antivirus programs miss because they analyze reputation and behavioral patterns rather than just file signatures.



Instead of disabling these protections, consider those warnings as an opportunity to re-examine the file using the methods mentioned above. And remember: Legitimate software rarely triggers multiple security warnings. If you see multiple layers of warnings, it's usually a clear indication that something is wrong.

You finished reading the article "**6 ways to check if a downloaded file is safe before using it.**" 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.
