PBST

Windows 10 is the most secure version of Windows ever used, with greatly improved antivirus, firewall, and disk encryption features — but it’s just not enough.

While Microsoft works hard to keep their users safe, hackers are still exploiting unique vulnerabilities only found in Windows computers, making Windows the most frequently hacked operating system in the world.

But most threats are easy to protect against, and it only takes a few minutes to make sure you’re keeping your PC secure.

How to Keep Your Windows 10 Computer Secure

1. Update Your Software Regularly

Keeping Windows and all your software up to date is a simple, yet vital part of protecting your computer from hackers.

Most updates are bug fixes and security patches that keep your operating system and software from providing a backdoor for hackers. The larger a piece of software is, the greater the likelihood that it will have vulnerabilities which a hacker can exploit.

Every time a hacker exploits a vulnerability, developers work to patch the vulnerability and update their product. Unfortunately, there are so many users on out-of-date versions of software that hackers can exploit the same vulnerabilities for years.

Windows 10 is designed to automatically update — all you need is an internet connection. However, different programs on your computer may not be so intuitive. Antivirus suites like Norton 360 use PC vulnerability scanners to ensure that all your software is up to date.

2. Always Research and Double-Check Your Downloads

Many malware infections can be attributed to user error. You can avoid a lot of security threats just by being cautious and researching the files and content you’re accessing.

A lot of hackers hide malware in seemingly legitimate downloads. Here are some simple steps you can take to ensure you’re not accidentally downloading a virus:

- Do a Google search to check how big the file you’re downloading is supposed to be.
- Look for more info about your downloads from forums and trustworthy websites.
- Look through the contents of a zipped folder before extracting the files.
- Use an antivirus to scan any files before you open them.

Taking extra time to double-check and research your downloads will save you a lot of stress — but a lot of malware downloads are very cleverly hidden — it can be very difficult to know if something is legitimate without running it on your computer. That’s why I also recommend you have a decent antivirus in case something gets past your defenses.

3. Protect Your Network with a Firewall

A firewall monitors the traffic coming in and out of your network, blocking incoming traffic from suspicious locations. This keeps malicious files and hackers from invading your computer through your internet connection. Windows's built-in firewall is pretty good, which you can access through the control panel.

While Windows Defender's firewall is pretty good, it's not nearly as powerful as most third-party options.

McAfee and Norton both include advanced threat detection in their firewalls, which allows them to determine new threats more effectively than Windows Firewall. These internet security tools also provide network health options to help you analyze the security of every device on your network.

4. Monitor Your PC with Windows Task Manager

If your computer is behaving strangely, you either have malware or a performance issue. When it comes to diagnosing computer problems, Windows Task Manager is the best place to start.

Task Manager tells you what programs are running on your computer, how much space they're taking up, and how much disk space is left on your hard drive.

Task Manager can be accessed by pressing Ctrl + Alt + Delete.

The Processes and Performance tabs are the most important diagnostic tools.

5. Avoid Dangerous Pop-Ups with an Ad Blocker

Advertisements are my least favorite part of the internet — they slow down my connection, waste my time, and they're often directly linked to malware and phishing websites.

Sketchy websites will use fake notifications or tricky pop-up ads to get you to download malware, visit a phishing site, or give your personal information to hackers. Ad blockers keep you out of these situations by blocking ads completely.

A lot of Chrome and Firefox users choose AdBlock Plus, which is a great ad blocking browser extension. However, Norton and Avira both offer ad blockers in their antivirus packages, which both block link tracking, so your browsing won't get traced between websites.

Having an ad blocker is a great way to reduce your risk of malware infection, especially if you're navigating to less secure websites.

6. Keep Your Browsing Private with a VPN, Especially on Public Wi-Fi

Using a VPN (virtual private network) is the best way to keep your internet use private — VPNs tunnel your data through an encrypted server, which ends up replacing your IP address with another (non-identifiable) IP address. Anybody tracking your browsing will only see the IP address of the anonymous server.

If your IP address is public, Big Data is probably selling your browsing history to marketers and businesses. A lot of governments and law enforcement officials track this history, and many laws force internet service providers and websites to share personal user information.

VPNs are especially important if you use public Wi-Fi networks. Public Wi-Fi networks can be set up by hackers who will spy on your usage once you connect to the network. A VPN makes it impossible to spy on your computer through a corrupted public Wi-Fi network.

VPNs are crucial tools for private browsing, public Wi-Fi security, and anonymous file-sharing. A lot of antivirus programs include VPNs in their security packages.

7. Use Device Encryption or Bitlocker to Protect Your Hard Drive

If your computer gets lost or stolen, the thief can easily remove your hard drive and access your files. Device encryption makes it almost impossible for anyone to get access to the information on your disk drive.

Encryption works by encoding your data with a super-complicated cipher, which can only be decoded by the computer that generated the encryption. Without your password, all of your data just appears as a string of random characters.

Windows Device Encryption is included on many Windows 10 Home machines. This feature can encrypt folders and files on command, as well as making disk partitions to store large amounts of encrypted data.

To see if you have this option enabled, click the Windows icon, then click Settings, then Update & Security.

Windows Device Encryption is strong, but users that upgrade to Windows 10 Pro get access to the BitLocker encryption tool. It encrypts all the data on your drive and includes a useful dashboard function to change settings.

Windows Device Encryption and BitLocker both use 256-bit AES encryption, which is the preferred encryption for banks, militaries, and governments around the world.

8. Use a Secure Password Manager with Two-Factor Authentication (2FA)

Once your passwords get hacked, your whole system becomes vulnerable. If you use the same password on different websites or your passwords aren't sufficiently complex, then your logins can be hacked into easily.

Password managers generate and autofill extremely complex and secure passwords between all your devices and browsers. The best password managers also offer useful extra features like encrypted storage and encrypted chat options — some even include a VPN!

All the best password managers support two-factor authentication (2FA), which requires you to enter both a password and a second form of verification to log into your password vault. This verification can be a fingerprint, face scan, USB stick, or temporary one-time password (TOTP) sent to your phone or smartwatch.

Windows Hello is the biometric authentication feature in Windows 10 — it syncs up with password managers like DashLane and Keeper so you can access your password vault with a simple face scan. This biometric 2FA makes it easy to keep your passwords as secure as possible.

9. Use a Secure Browser

Microsoft Edge is a big improvement over the famously terrible Internet Explorer browser, but it's just not good enough. You should switch to Mozilla Firefox or Google Chrome — they both offer better protection against phishing sites and malicious web scripts than Edge.

There's one more way for Windows users to ensure their browsers can't be a source for malware infection — Windows 10 Pro now includes the Sandbox tool. This tool allows programs to run in a virtual machine — sandboxed programs can't access any of your system files, and any changes they make disappear when you close the virtual machine.

I run Chrome in Sandbox, which allows me to navigate wherever I want on the web with zero risk — any dangerous web script or attempted system invasion is cut off the moment I close Sandbox.

10. Close Your Back Door by Uninstalling Flash ASAP

Adobe Flash Player used to be the most popular media player on the internet — for users and hackers alike. Hackers had so much success using Flash as a backdoor into people's systems that it needed security updates almost weekly. Nowadays, a lot of hackers use fake Flash updates to trick users into installing viruses on their computers!

HTML5 made Flash obsolete a few years ago, and Adobe announced in 2019 that it would be completely phasing out Flash in 2020. There is no longer any reason to have Flash on your computer — it's basically just an avenue for hackers to infiltrate your machine.

Uninstalling Flash on Windows 10 is simple. While you can't uninstall Flash using the Windows Uninstall function, Adobe offers an uninstaller app for Flash on their website. Just download the app and run Adobe's uninstaller to remove it from your computer.

I also recommend that you change your browser settings and disable the Flash plugin. In Chrome, do this by selecting the Privacy and Security tab in Settings, then select Site Settings. Click on the Flash option and tell Chrome to block websites from running Flash.

11. Download an Antivirus

Even if you follow every precaution, malware can still find its way onto your PC. Antivirus software can be seen as the last line of defense against malware.

The best antivirus products have a better malware detection rating than Windows Defender, plus a huge range of helpful features. Every program has something that sets it apart from the rest — here are some of my favorite antivirus programs:

- Norton — Has a 100% malware detection rating, good VPN, identity theft protections, and comprehensive parental controls.
- Avira — Powerful antivirus protection as well as system speedup tools to boost performance on slower PCs.
- McAfee — Comprehensive internet security package as well as the best mobile anti-theft protections on the market.
- Bitdefender — Cloud-based scanner protects your system without using up disk space (one of the best lightweight antivirus options out there).

Now You Know How to Keep Your PC Safe

Cybersecurity is more than just a set of practices and software tools, it's a state of mind. Just like I wouldn't leave my front door unlocked and invite untrustworthy people into my home, I don't go on the internet without these essential protections.

There are a lot of hackers out there, but they mostly prey on the unprepared. By following these tips and staying educated about the latest cybersecurity threats, you can ensure your computer's health and well-being for years to come.