Your computer is not as secure as you think

Just because you have active antivirus software and a password doesn't mean your computer is invulnerable. You could be leaving your computer vulnerable without even realizing it!

Just because you have active antivirus software and a password doesn't mean your computer is invulnerable. You could be leaving your computer vulnerable without even realizing it!

1. Default settings are not always safe

While default settings can be convenient, they are not good for security. For example, default router settings make your home network vulnerable to hacking. Your router has a default *admin* name and password that are vulnerable to attack. After all, the default login credentials can be easily found online. Other router settings, such as remote management, WPS, and Universal Plug and Play (UPnP), should also be disabled. These helpful features come at a cost to your network security.

Likewise, native browser settings can cause problems. For overall security, you should keep your browsing data private. This can include disabling third-party cookies and setting your browser to not sync data to protect your passwords. Doing so will make your browsing experience worse, but at least it will keep you private.

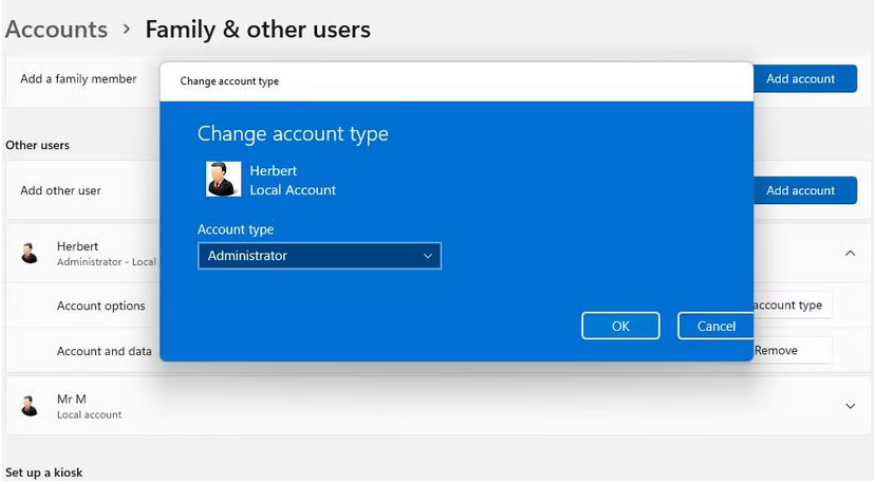
2. Updates are more important than you think

You've probably skipped system updates many times because they were inconvenient. While this may not seem like a big deal, it could leave you open to a cyberattack.

System or software updates often come with security patches to fix vulnerabilities and bugs that hackers can use to gain access to your system. These updates are often time-sensitive because they address vulnerabilities that most criminals already know about. These guys are after easy targets, and there's nothing easier than targeting targets with outdated software.

The same goes for running old apps that aren't compatible with the latest security features, or running devices with outdated firmware. You may be sticking with Windows 7 because you like it, but it's an outdated operating system that hasn't been officially supported for nearly four years, and is almost old enough to run and vulnerable to exploits.

3. Use admin account for daily tasks



Using an admin account for your computer is generally like leaving your car keys with a known thief. Admin accounts can often make changes to the system without running into any issues, such as warnings that they may cause damage or other problems. As you can imagine, malware developers like admin accounts because it makes it easier to infect computers without alerting the user.

On Windows, it's pretty easy to avoid this fate by creating a standard account, which you use for your daily tasks and your free time. A standard account has less access to Windows settings, and while that doesn't mean you won't get any malware, it can help isolate the problem.

4. Passwords aren't as secure as you think

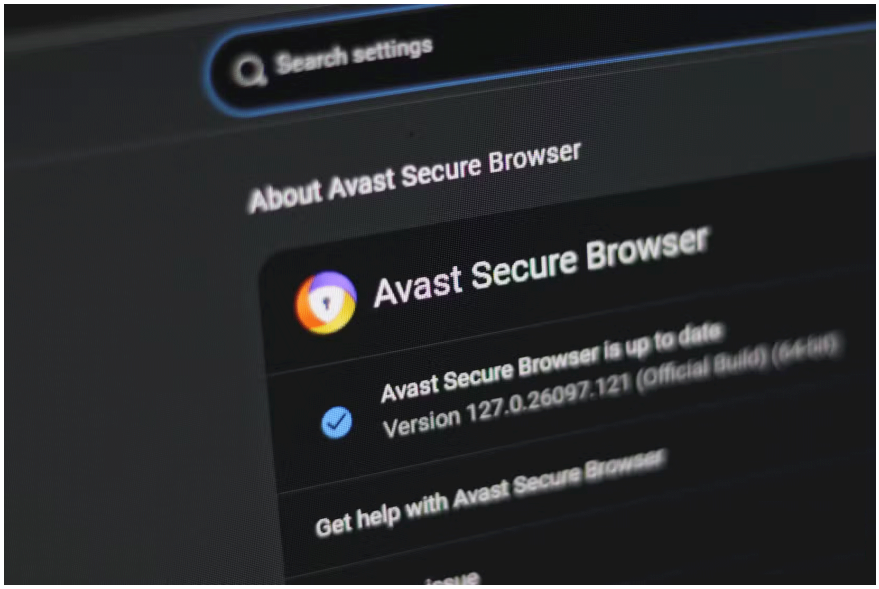
There are many myths about password security. For example, using one strong password across multiple websites may seem like a good idea. After all, a strong password seems insurmountable. However, if a cybercriminal gets a hold of it, they will try to access any accounts involved. Therefore, it is much safer to create a different password for each account.

Even if a site seems to have solid password rules, there's still a chance that something could go wrong for you. Suppose there's a minimum length requirement: A potential hacker would have an unfair advantage because they only need to work out combinations that fit the length requirement. In other words, the password could become as easy to guess as a dog's name with a bunch of numbers added just to make it long enough.

Your passwords may not be strong enough because you're reusing them across multiple accounts or choosing something new and simple that you can't remember. You can avoid these problems (and make your passwords better) by using a password manager. Use a random password generator to generate hard-to-crack passwords for all your accounts and store them for convenience.

5. You may be leaking private data

Cookies and browser fingerprinting are implemented to improve the user experience. However, hackers can exploit this level of information. For example, browser fingerprinting creates a unique 'fingerprint' for each user, allowing companies to track them across websites.



However, hackers can also build browser fingerprinting profiles, which may not infect your device immediately. You may visit a compromised website to collect information. The information is sent to the hacker, who can then use it to find other vulnerabilities in your system. Similarly, many HTML5 features can be exploited to capture browser information that requires a specific vulnerability on your machine, while cookies can help build an image of the websites you visit.

Installing one of the more secure browsers is a good start. Firefox, for example, has implemented protection that randomizes your fingerprint, making it harder to create unique profiles.

Sometimes, you can accidentally give away your information by giving too many permissions to an app. While this is usually a bigger problem on mobile devices, desktop apps can access your registry, personal files, and other programs. Not only is this predatory, it can be dangerous. If an app is compromised, a stealthy hacker can have free access to most of your data.

6. You think, 'It won't happen to me.'

Most people simply don't believe that bad things can happen to them, even when danger is lurking. Most people think they are too small a target and therefore don't take security seriously. This is exactly what hackers are looking for.

Be aware that most cyber attacks are opportunistic and automated. Hackers often crack passwords by using common passwords across multiple websites. The people behind these attacks don't know who you are and you just happen to be the victim.

No matter how normal you think you are, your data is valuable. Hackers can sell it on the dark web, use it to steal your identity and money, threaten you, and do anything else that will allow them to make money.