Cyber Security

12 Ways to Secure Your Computer From Hackers

Cybercrime is serious business and is costing the economy **$3.2M every minute**. WireLite Technologies wants our customers to be safe when online.

This guide is the best first step to protect you against Cybercrime.

Cybercrime is a **People issue**, technology does what people (good or bad) tell it to do.

1. Use a firewall.

The major computer operating systems have built-in firewalls, software designed to create a barrier between your information and the outside world. Firewalls prevent unauthorized access to your network. The first thing to do with a new computer (or the computer you now use) is to make sure the firewall is enabled before you go online. However, you can also purchase a hardware firewall from companies like Cisco, Sophos or Fortinet, depending on your broadband router, which also has a built-in firewall that protects your network. If you have a larger business, you can purchase an additional business networking firewall.

2. Install antivirus software.

Computer viruses, keyloggers and Trojans are everywhere. Antivirus programs such as Bitdefender, Kaspersky, Trend Micro, AVG, and Avast immunize your computer against unauthorized code or software that threatens your operating system. Viruses have various effects that may be easy to spot: They might slow your computer to a halt or delete key files. Antivirus software plays a major role in protecting your system by detecting real-time threats to ensure your data is safe. Some advanced antivirus programs provide automatic updates, further protecting your machine from the new viruses that generate every day. After you install an antivirus program, don't forget to use it. Run or schedule regular virus scans to keep your computer virus-free.

3. Install an anti-spyware package.

Spyware is a special kind of software that secretly monitors and collects personal or organizational information. It is designed to be hard to detect and difficult to remove, and tends to serve up unwanted ads or search results to direct you to certain websites. Some spyware records every keystroke to gain access to passwords and other financial information. Anti-spyware concentrates exclusively on this part of the nuisance spectrum but is often included in major antivirus packages like Webroot, McAfee and Norton. Anti-spyware packages provide real-time protection by scanning all incoming information and blocking threats.

4. Use complex passwords.

Using secure passwords is the most important way to prevent illegal intrusions onto your computer network. The more secure your passwords, the harder it is for a hacker to invade your system. Use a secure Password generator like: https://passwordsgenerator.net/ More secure often means longer and more complex: Use a password that has at least eight characters and a combination of numbers, upper- and lowercase letters, and computer symbols. Hackers have an arsenal of tools to break short, easy passwords in minutes. Don't use recognizable words or combinations that represent birthdays or other information that can be connected to you. Don't reuse passwords either; if you have too many passwords to remember, consider using a password manager like Dashlane, Sticky Password, LastPass or Password Boss.

5. Keep your OS, apps and browser up to date.

Always install new updates to your operating systems. Most updates include security fixes that prevent hackers from accessing and exploiting your data. The same goes for your favorite apps. Today's web browsers are increasingly sophisticated, especially in privacy and security. Be sure to review your browser security settings in addition to installing all new updates. For example, you can use your browser to prevent websites from tracking your movements, which increases your online privacy.

6. Ignore spam.

Beware of email messages from unknown parties, and never click on links or open attachments that accompany them. Spam-catchers have upped their game in recent years and become pretty good at catching the most egregious spam. But phishing emails that mimic your friends, associates and trusted businesses like your bank have proliferated, so keep your antenna tuned to anything that looks or sounds dodgy.

7. Back up your computer.

If your business is not already backing up your hard drive, then data loss is still a threat. Backing up your information is critical in case disaster strikes and hackers do get through and trash your system. Always be sure you can rebuild as quickly as possible after suffering any data breach or loss. Backup utilities built into the Mac (Time Machine) and Windows (File History) are good places to start. Purchasing an external backup hard drive like; Western Digital, Seagate and CalDigit assure there is enough space for these utilities to operate properly. Keep your backup drive safe.

8. Operate your PC as a standard user.

The first step to elevate your security is to remove the ability of Cyber-attacks access to **Administrator privileges** on your PC. Out of the box PC's or new installs of an Operating System default to Administrator privileges. Adding a user account with "standard user privileges" for your day to day PC usage will greatly enhance your Cyber security. When you login to your PC as a user with Administrator privileges, any operations you do will also run with Administrator privileges. So if your PC is infected, it won't ask for permission to copy, delete or change anything on your PC. It could copy your emails, banking details, login passwords or other sensitive details and send them back to the Cyber criminals. Create a new user account with standard user privileges and **avoid using the Administrator account for day to day usage**.

9. Avoid "Suspect" web sites.

Effective methods used by hackers is to infect websites with malicious code. This code resides on the web server and when a user visits the website, the hackers code is downloaded on to your PC. So simply said, just visit an infected site and your machine could be compromised.

10. Secure your network.

If you've got a new router, chances are it comes with no set security. Always log in to the router and set a password using a secure, encrypted setup. This prevents intruders from infiltrating your network and messing with your settings.

11. Use two-factor authentication.

Passwords are the first line of defense against computer hackers, but a second layer boosts protection. Major online companies like Facebook, Google, Apple and Microsoft let you enable two-factor authentication, which requires you to type in a numerical code in addition to your password when logging in. This hardens your account to the outside world.

12. Use encryption.

Even if someone is able to steal your data or monitor your internet connection, encryption can prevent hackers from accessing any of that information. You can encrypt your Windows or macOS hard drive with BitLocker or FileVault, encrypt any USB flash drive that contains sensitive information, and use a VPN to encrypt your web traffic. Only shop at encrypted websites – you can spot them immediately by the "https" in the address bar accompanied by a closed padlock icon.

Bottom line

If only internet thieves used their creative talents to earn an honest living, we wouldn't have to take so many precautions to lock down and harden our computer systems. Until that happens a combination of hardware and personal vigilance, will remain the barrier between you and online predators.

Happy Safe computing.