

10 Easy Steps to Secure Your Computer

By Jen Heller Meservey

They're out there: Hackers, spammers, fishers, scammers, identity thieves, and viruses. Every day they work to find new ways to crack your passwords, break into your accounts, steal your credit card numbers, and just generally wreak havoc on your hard drive, but you don't have to swear off the Internet for good. Here are ten ways you can secure your computer and keep your information safe.

1. **Install anti-virus software.** These days, most PCs come with a free trial of anti-virus software already installed. Often computer users will let their free trial expire without renewing it or installing something else. Don't leave your computer without virus protection! While top of the line anti-virus software like Norton and McAfee are best, if you're short on funds you can still get adequate virus protection with a free program like AVG (www.avg.com) or Avast (www.avast.com). Whatever you use, make sure your anti-virus software doesn't expire and leave your computer susceptible to viruses.

TIP: If your PC came with a free trial of an expensive anti-virus program like Norton or McAfee, use it as long as you can. This will give you premium protection for the trial period, after which you can install a free program like AVG or Avast.

2. **Update, update, update!** You know those little notifications that pop up in the bottom-right corner of the screen telling you a new update is available? Don't ignore them! It is very important that you keep your operating system, your anti-virus software, and all other programs up-to-date in order to keep your computer secure. New viruses and security loopholes are discovered every day, and if you don't have the latest updates, your computer could be at risk. Install updates regularly to keep your computer protected.

TIP: Check the settings of your anti-virus program and set it to install updates automatically, so you don't even have to worry about clicking on those little notifications.

3. **Run regular virus scans.** While your anti-virus program will typically run in the background, always protecting you from intrusions, occasionally viruses may slip through. That's why it's important to run regular virus scans to keep your computer protected. Most anti-virus programs allow you to create a schedule for regular scans. It is recommended that you scan your entire hard drive weekly for the best protection against viruses.

TIP: Schedule your scan to take place at a time when you know you won't be using your computer, so the scan doesn't slow you down.

4. **Use Windows Firewall.** Windows comes with a built-in firewall that can help protect your computer from unauthorized access while you're online. Check your Control Panel to make sure you have Windows Firewall turned on for all of the connections you use.

TIP: Be sure to add your anti-virus program to the Windows Firewall's list of "exceptions," so that it can update without being blocked.

5. **Secure your wifi connection.** It's easy to set up your home wireless network as "open," so you don't have to worry about entering a password when you connect your devices, but this can

leave your connection vulnerable to intrusion, and slow it down when neighbors decide to log on and get some free Internet access. Make sure your wireless network has a password that only you know.

TIP: Whenever you connect a new device to your wireless network, set it to remember the password. That way, you won't have to enter it every time you connect.

6. **Don't login as "administrator."** While it's easy to just login to your computer's administrator account so you can install and uninstall programs without switching users, this leaves your computer vulnerable to any viruses, spyware, or malware that may want to install themselves on your hard drive. It's best to create a separate account with limited access, and use only that account to access the Internet. Users with limited access cannot install new programs, or make system changes, which means intruders can't do those things either.

TIP: If having to switch users gets to be a pain, just remember your computer's administrator password. Many programs will install when you enter this password, so you won't have to switch accounts.

7. **Use strong passwords.** Whether you're creating a password to login to your computer, your e-mail, or your Facebook account, you need to make sure you're using strong, complex passwords. It's best to use a password which includes at least one of each of the following: lower case letter, upper case letter, number, and special character. For example, if your birthday is March 8th, don't just use "0308," try something like "M@rch08."

TIP: If you find it hard to remember all of your various passwords, don't write them down. Use a free online password manager like Passpack (www.passpack.com) to keep your passwords secure.

8. **If you're away from home, lock your computer when you're not using it.** Whether you're at work, an Internet café, library, or coffee shop, it's important to lock your computer if you happen to walk away from it. In Windows, you can easily do this by pressing "Ctrl+Alt+Del" and then clicking "Lock Computer." Once locked, the computer will require a password for access.

TIP: Set your screensaver to lock your computer automatically, and make sure the screensaver comes on after a short interval, like one minute. This way, if you forget to lock your computer, your screensaver will do it for you.

9. **Block spam e-mails.** Spam e-mail messages can contain viruses, fake links, and other scams that may seem legitimate, and can be tempting to click. When using an e-mail client like Microsoft Outlook, it's best to block spam messages with a free spam blocking program, like Mailwasher (www.mailwasher.net), or SPAMfighter (www.spamfighter.com). Many web-based e-mail providers, like Gmail and Yahoo, include spam blocking in their webmail systems. Check with your e-mail provider to make sure that spam blocking is in effect on your account.

TIP: If you spot any spam messages, make sure you mark them as spam in whatever spam blocker you're using, to help the program "learn" to block similar messages in the future.

10. **Be careful what you click.** No matter how strong your spam blocker is, occasional spam and scam messages can still find their way to your inbox. That's why it's important to be careful what you click. Be wary of messages from e-mail addresses you don't recognize. Don't click on links in these messages, and definitely don't open attachments.

TIP: Some anti-virus programs give you the option to scan e-mails and attachments for viruses. Turn on this setting to ensure that all of your e-mail messages are virus-free before you open them.

Follow these ten steps and protect your computer from viruses, spyware, malware, hackers, and identity theft, so you can browse the web worry-free.