Before You Connect a New Computer to the Internet

Original release date: December 15, 2015 | Last revised: October 29, 2018

Why is computer security important?

Because computers play such critical roles in our lives, and because we input and view so much personally identifiable information (PII) on them, it's imperative to implement and maintain computer security. Strong computer security ensures safe processing and storage of our information.

How can I improve my computer's security?

The following are important steps you should consider to make your computer more secure. While no individual step will eliminate all risk, when used together, these defense-in-depth practices will strengthen your computer's security and help minimize threats.

- **Secure your router.** When you connect a computer to the internet, it's also connected to millions of other computers—a connection that could allow attackers access to your computer. Although cable modems, digital subscriber lines (DSLs), and internet service providers (ISPs) have some level of security monitoring, it's crucial to secure your router—the first securable device that receives information from the internet. Be sure to secure it before you connect to the internet to strengthen your computer's security. (See Securing Your Home Network for more information.)
- **Enable and configure your firewall.** A firewall is a device that controls the flow of information between your computer and the internet. Most modern operating systems (OSs) include a software firewall. The majority of home routers also have a built-in firewall. Refer to your router's user guide for instructions on how to enable your firewall and configure the security settings. Set a strong password to protect your firewall against unwanted changes. (See Understanding Firewalls.)
- **Install and use antivirus software.** Installing an antivirus software program and keeping it up-to-date is a critical step in protecting your computer. Many types of antivirus software can detect the presence of malware by searching for patterns in your computer's files or memory. Antivirus software uses signatures provided by software vendors to identify malware. Vendors frequently create new signatures to ensure their software is effective against newly discovered malware. Many antivirus programs offer automatic updating. If your program has automatic updates, enable them so your software always has the most current signatures. If automatic updates aren't offered, be sure to install the software from a reputable source, such as the vendor's website. (See Understanding Anti-Virus Software.)
- **Remove unnecessary software.** Intruders can attack your computer by exploiting software vulnerabilities, so the fewer software programs you have installed, the fewer avenues there are for potential attack. Review the software installed on your computer. If you don't know what a software program does, research the program to determine whether or not the program is necessary. Remove any software you feel isn't necessary after confirming it's safe to remove. Back up important files and data before removing

unnecessary software to prevent accidentally removing programs that turn out to be essential to your OS. If possible, locate the installation media (e.g., CD) for the software in case you need to reinstall it.

- **Modify unnecessary default features.** Like removing unnecessary software, modifying or deleting unnecessary default features reduces attackers' opportunities. Review the features that are enabled by default on your computer, and disable or customize those you don't need or don't plan on using. As with removing unnecessary software, be sure to research features before modifying or disabling them.
- **Operate under the principle of least privilege.** In most instances of malware infection, the malware can operate only using the privileges of the logged-in user. To minimize the impact of a malware infection, consider using a standard or restricted user account (i.e., a non-administrator account) for day-to-day activities. Only log in with an administrator account—which has full operating privileges on the system—when you need to install or remove software or change your computer's system settings.
- **Secure your web browser.** When you first install a web browser on a new computer, it will not usually have secure settings by default, you will need to adjust your browser's security settings manually. Securing your browser is another critical step in improving your computer's security by reducing attacks that take advantage of unsecured web browsers. (See Securing Your Web Browser.)
- **Apply software updates and enable automatic updates.** Most software vendors release updates to patch or fix vulnerabilities, flaws, and weaknesses (bugs) in their software. Intruders can exploit these vulnerabilities to attack your computer. Keeping your software updated helps prevent these types of infections. (See Understanding Patches and Software Updates.) When setting up a new computer, go to your software vendors' websites to check for and install all available updates. Many OSs and software programs have options for automatic updates. Enable automatic updates if they are offered; doing so will ensure your software is always updated, and you won't have to remember to do it yourself. Only download software updates directly from a vendor's website, from a reputable source, or through automatic updates.

What are some additional best practices I can follow?

There are other simple practices you can follow to improve your computer's security.

- **Use caution with email attachments and untrusted links.** Malware is commonly spread by users clicking on a malicious email attachment or a link. Don't open attachments or click on links unless you're certain they're safe, even if they come from a person you know. Be especially wary of attachments with sensational names, emails that contain misspellings, or emails that try to entice you into clicking on a link or attachment (e.g., an email with a subject that reads, "Hey, you won't believe this picture of you I saw on the internet!"). (See Using Caution with Email Attachments.)
- **Use caution when providing your information.** Emails that appear to come from a legitimate source and websites that appear to be legitimate may be malicious. An example is an email claiming to be sent from a system administrator requesting your password or other sensitive information or directing you to a website that requests your information. Online services (e.g., banking, ISPs, retailers) may request that you change your password, but they will never specify what you should change it to or ask you what

it is. If you receive an email asking you to change your password, visit the site yourself instead of clicking on any link provided in the email. (See Avoiding Social Engineering and Phishing Attacks.)

- **Create strong passwords.** Use the strongest, longest password or passphrase permitted. Don't use passwords that attackers can easily guess, like your birthday or your child's name. Attackers can use software to conduct dictionary attacks, which try common words that may be used as passwords. They also conduct brute force attacks, which are random password attempts that run until one is successful. When setting security verification questions, choose questions and answers for which an internet search would not easily yield the correct answer (e.g., your pet's name). (See Choosing and Protecting Passwords.)

Authors
NCCIC