

Before You Connect a New Computer to the Internet

Computers are an important part of everyday life. In order to keep your computer and information secure, it is important to properly set up your computer before connecting to the Internet.

Why Should I Care About Computer Security?

Computers help us maintain our financial, social, and professional relationships. We use them for banking and bill paying, online shopping, connecting with our friends and family through email and social networking sites, researching data posted on the Internet, and so much more. We rely heavily on our computers to provide these services, yet we sometimes overlook our need to secure them. Because our computers play such critical roles in our lives, and we input and view so much personally identifiable information (PII) on them, it's imperative to maintain computer security that ensures the safe processing and storage of our information.

How Do I Improve the Security of My Home Computer?

Following are important steps you should consider to make your home computer more secure. While no individual step will eliminate your risk, together these defense-in-depth practices will make your home computer's defense stronger and minimize the threat of malicious exploit.

1. *Connect to a Secure Network*

Once your computer is connected to the Internet, it's also connected to millions of other computers, which could allow attackers access to your computer. Information flows from the Internet to your home network by first coming into your modem, then into your router and finally into your computer. Although cable modem, digital subscriber line (DSL), and internet service providers (ISP) purport 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 improve your computer's security (See [Securing Your Home Network](#) for more information).

2. *Enable and Configure a Firewall*

A firewall is a device that controls the flow of information between your computer and the Internet, similar to a router. Most modern operating systems include a software firewall. In addition to the operating system's firewall, the majority of home routers have a firewall built in. Refer to your user's guide for instructions on how to enable your firewall. Once your firewall is enabled, consult the user's guide to learn how to configure the security settings and set a strong password to protect it against unwanted changes. (See [Understanding Firewalls](#) for more information.)

3. *Install and Use Antivirus and Antispyware Software*

Installing an antivirus and antispyware software program and keeping it up to date is a critical step in protecting your computer. Many types of antivirus and antispyware software can detect the possible presence of malware by looking for patterns in the files or memory of your computer. This software uses virus signatures provided by software vendors to look for malware. Antivirus vendors frequently create new signatures to keep their software effective against newly discovered malware. Many antivirus and antispyware programs offer automatic updating. Enable that feature 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, like the vendor's website or a CD from the vendor. (See [Understanding Anti-Virus Software](#).)

4. *Remove Unnecessary Software*

Intruders can attack your computer by exploiting software vulnerabilities (that is, flaws or weaknesses), so the less software you have installed, the fewer avenues for potential attack. Check the software installed on your computer. If you don't know what a software program does and don't use it, research it to determine whether it's necessary. Remove any software you feel isn't necessary after confirming it's safe to remove the software.

Back up important files and data before removing unnecessary software in case you accidentally remove software essential to the operating system. If possible, locate the installation media for the software in case you need to reinstall it.

5. *Modify Unnecessary Default Features*

Like removing unnecessary software and disabling nonessential services, modifying unnecessary default features eliminates opportunities for attack. Review the features that came enabled by default on your computer and disable or customize those you don't need or plan on using. As with nonessential services, be sure to research these features before disabling or modifying them.

6. *Operate Under the Principle of Least Privilege*

In most instances of a malware infection, the malware can operate only under the rights of the logged-in user. To minimize the impact the malware can have if it successfully infects a computer, consider using a standard or restricted user account for day-to-day activities and only logging in with the administrator account (which has full operating privileges on the system) when you need to install or remove software or change system settings from the computer.

7. *Secure Your Web Browser*

Web browsers installed on new computers usually don't have secure default settings. Securing your browser is another critical step in improving your computer's security because an increasing number of attacks take advantage of web browsers. (See [Securing Your Web Browser](#).)

8. *Apply Software Updates and Enable Future Automatic Updates*

Most software vendors release updates to patch or fix vulnerabilities, flaws, and weaknesses (bugs) in their software. Because intruders can exploit these bugs to attack your computer, keeping your software updated is important to help prevent infection. (See [Understanding Patches](#).)

When you set up a new computer (and after you have completed the previous practices), go to your software vendors' websites to check for and install all available updates. Enable automatic updates if your vendors offer it; that will ensure your software is always updated, and you won't have to remember to do it yourself. Many operating systems and software have options for automatic updates. As you're setting up your new computer, be sure to enable these options if offered. Be cautious, however, because intruders can set up malicious websites that look nearly identical to legitimate sites. Only download software updates directly from a vendor's website, from a reputable source, or through automatic updating.

9. *Use Good Security Practices*

You can do some simple things to improve your computer's security. Some of the most important are:

- **Use caution with email attachments and untrusted links.** Malware is commonly spread by people clicking on an email attachment or a link that launches the malware. Don't open attachments or click on links unless you're certain they're safe, even if they come from a person you know. Some malware sends itself through an infected computer. While the email may appear to come from someone you know, it really came from a compromised computer. 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 (for example, an email with a subject like 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 sensitive information.** Some email or web pages that appear to come from a legitimate source may actually be the work of an attacker. 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 requesting that information. While Internet service providers may request that you change your password, they will never specify what you should change it to or ask you what it is. (See [Avoiding Social Engineering and Phishing Attacks](#).)
- **Create strong passwords.** Passwords that have eight or more characters, use a variety of uppercase and lowercase letters, and contain at least one symbol and number are best. Don't use passwords that people can easily guess like your birthday or your child's name. Password detection software can conduct dictionary attacks to try common words that may be used as passwords or conduct brute-force attacks where the login screen is pummeled with random attempts until it succeeds. The longer and more complex a password is, the

harder these tools have to work to crack it. Also, when setting security verification questions, choose questions for which it is unlikely that an Internet search would yield the correct answer. (See [Choosing and Protecting Passwords](#).)

Author

US-CERT Publications