



► PROTECT Your Computer

Online safety and security begin with you

The Internet is a global network that connects most of the world's computers and an increasing number of smart phones and other devices. It offers a seemingly limitless universe of information, images, and opportunities.

Yet these benefits come with some risks. Just by logging on to the Internet, you can be exposed to security threats that might cripple or control your computer, compromise your privacy, or destroy your valuable data.

► Top threats to computer security

The leading threats to the security of your computer come from four types of malicious software:

- **Viruses** are software programs designed to invade computers and to copy, damage, or delete data.
- **Worms** are sophisticated viruses that can reproduce themselves and spread to other computers without your interaction.
- **Trojans**, named for the Trojan horse, are viruses that pretend to be helpful programs while destroying your data, damaging your computer, and stealing personal information.
- **Spyware** is software that tracks your online activity. Spyware may bombard you with pop-up advertising, collect your personal information, or change the settings on your computer without your knowledge or consent.

To help protect your computer, follow the steps below. For details, visit www.staysafe.org.

► Keep your firewall turned on

A firewall helps to protect your computer by placing a protective barrier between your computer and the Internet, camouflaging it from hackers and malicious software, such as viruses and worms.

- The firewall operates as a kind of security checkpoint that information must pass through before it can enter or leave your computer.
- A firewall also helps to prevent software on your computer from accepting unauthorized updates or changes sent over the Internet.

► Keep your software updated

One of the most important things you can do to help protect your computer is also one of the easiest: keep your operating system and other software up-to-date.

- Hackers work tirelessly to exploit weaknesses in software, and new security threats emerge every day. That's why software companies work even harder to help keep your computer safe with updates, and it's why you should install updates.
- If your operating system includes an automatic update feature, turn it on to make sure you get the latest updates as soon as they are issued. Check other software programs and software company Web sites for updates.

► Use up-to-date antivirus software -----

Antivirus programs scan everything that goes into your computer—including e-mail, discs, and data files—searching for thousands of known viruses.

- Antivirus software requires regular signature updates to help protect against emerging threats. Installing antivirus software without updating it is like buying home insurance but not making the payments. Keep your antivirus software current by subscribing to an antivirus service and automatically downloading the latest updates.

► Use up-to-date antispyware software -----

Antispyware programs monitor your computer, looking for known spyware and watching for programs that try to install without your knowledge or permission. When antispyware programs find something, they warn you and help you take action against the unwanted software.

- As with antivirus software, keep your antispyware software current, and automatically download the latest updates.

In addition to using a firewall and keeping your operating system, antivirus, and antispyware software updated, take these steps to help protect your computer:

► Think before you click -----

Clicking the wrong link or attachment can expose your computer to spyware, viruses, or ads that could clutter your screen and slow your computer.

- Be very cautious with attachments or links in e-mail or instant messages. If you know the sender, but the message looks suspicious, check with the sender before you proceed. If they didn't send the message, delete the e-mail or close the IM window.
- Think twice before you click pop-up windows or banner ads.
- Never click *Agree*, *OK*, or *I accept* to get rid of a pop-up ad, an unexpected warning, or even an offer to remove spyware. Instead, close the window by clicking *X* in the upper-right corner or by pressing **ALT + F4** on your keyboard.
- Download software only from Web sites you trust. File-sharing programs and sites that offer "free" music, movies, games, and other information are notorious for including unwanted software in downloads.

► Back up your files -----

No security method is completely foolproof. So it's important to back up critical files regularly, before you get hit with a problem.



► **Helpful Resources:**
www.staysafe.org

 staysafe.org