

Computers and the Internet have changed our world. We now can work, learn, play, socialize, shop and manage our daily lives online, without leaving the comfort of our own homes.

But not everyone we interact with online is trustworthy. Some people use the Internet to anonymously harass or annoy others, to damage computer systems or data, or even commit crimes.

Fortunately, some simple steps can help you avoid becoming a victim. By knowing what to look for, taking precautions, and using protective tools, you can enjoy the benefits of the Internet while keeping yourself, your family, your computer data and your personal information safe and secure.

Potential Risks for Internet Users

Depending on how you use the Internet, you may be taking unnecessary risks. You might be at risk of identity theft (when someone steals and uses your personal information, perhaps to open new credit accounts); data theft or damage; or personal safety threats (sometimes called cyberstalking or cyberbullying). Here are some of the ways crooks and con artists find victims online:

- **Phishing**—an attempt to “hook” you into revealing your personal and confidential information by sending bogus emails that appear to come from a legitimate business.
- **Spam**—unwelcome email and instant messages, which may offer questionable goods for sale or a promise of financial rewards if you give the sender money.
- **Malware**—malicious software (spyware, Trojans, viruses and worms) that can be remotely installed on your computer, allowing the person who controls the malicious software to steal, damage or delete your files and other data.
- **Transactions that are not secure**—sites that don’t have secure payment forms, or companies that store debit and credit card information without proper safeguards, may give crooks the opportunity to intercept your personal information.
- **Social networking**—users may be at risk if they reveal too much personal information, or if they agree to physically meet people they first met online. Some social networking

sites might even compromise sensitive personal information.

Protecting Your Computer and Data

There are many ways that someone can gain access to your personal information. Fortunately, there are also many ways for you to protect yourself.

- **Use a firewall.** A firewall is a virtual barrier between your computer and the Internet. Everything coming into or leaving your computer must go through the firewall, which blocks anything that doesn’t meet specific security criteria. Before purchasing separate firewall hardware or software, check your operating system (or OS) to see if there is a built-in firewall and whether it is turned on. (Mac OS X or Windows Vista are two widely used operating systems.)
- **Install antivirus software.** Antivirus software scans everything that goes into your computer, looking for known viruses. Because new viruses are created all the time, you should update your antivirus software regularly.
- **Install antispyware software.** Spyware is software that tracks your computer activity, gathering information without your knowledge. Antispyware software blocks or removes spyware. Some antivirus products include antispyware features.
- **Use a spam filter.** Most Internet service providers (ISPs) and email programs now include an automatic spam filter, which reduces the number of unwanted email messages that make it to your inbox. Delete, without opening, any spam or “junk mail” that gets through the filter.
- **Perform timely updates.** Computer and software companies frequently update their programs to include protection against the newest security threats. So, simply updating your operating system and software whenever new versions become available gives you an added measure of security. If available, activate automatic security updates so you will be alerted when updates are issued.
- **Create strong passwords.** A strong password includes a seemingly random string of letters, numbers and symbols. It should never include personal information, such as your birth date, address or pet’s name. Include at least eight

characters in your passwords. Longer passwords are harder for intruders to infer or decipher.

- **Secure your wireless network.** Leaving your network “unlocked” means that anyone within range of your wi-fi signal can access it—and possibly capture the data you send and receive. Securing your wireless network can be as simple as creating a strong password for your router and enabling its built-in encryption tool.

A Special Note About Older Computers

If you have an older computer, you may no longer receive updates and security “patches,” and the manufacturer probably does not offer support for your computer. New versions of browsers have important security features that may not run on older operating systems. Firewalls are relatively new and are activated by default by the manufacturer on newer computers. But firewalls may not be activated on older machines. As a result, older computers with “always on” high-speed Internet connections may be at risk for security and privacy breaches.

Protecting Your Privacy from Online Marketers

Guarding your personal information while on the web not only protects you from dishonest people, it reduces your exposure to nuisances such as unwanted marketing messages.

A simple but effective way to maintain your privacy is to reveal as little as possible about yourself at unfamiliar sites until you have decided you want to establish a relationship. Any time you fill out a form, enter an online contest, or otherwise submit information electronically, that information could potentially be used for marketing purposes—by the company whose site you are visiting, or by a third party that buys the information. Read the “Privacy Policy” for sites you interact with to make sure they will not sell or trade your contact information.

You may also want to manage your “cookies.” Cookies can be placed on your computer’s hard drive after you visit a website. The cookie tells the host site things like which pages you visited, and what you placed in your shopping cart. That information is recorded whenever you visit the site. Companies sometimes

use cookies to target their marketing efforts. If you don’t want the site to retain any of your information or recognize you as a repeat visitor, set your Internet browser to delete your cookies automatically whenever you exit the browser. You can also set your browser to not accept cookies, but that may restrict you from visiting certain sites.

To limit the number of unwanted messages in your primary email inbox you can create an alternate email address that you use for certain online activities. There are many free email services to choose from.

Ignore and delete spam completely. Do not respond, even to unsubscribe, because your response confirms that the address is “live.”

Legitimate companies will have a privacy policy. The policy should clearly state when and how the company might use your information. Leave the site if you are not satisfied that your privacy will be protected. Look for “trust mark” logos, such as TRUSTe, that certify trustworthy privacy policies.

If you have children, instruct them not to reveal private information at websites they visit. (The Children’s Online Privacy Protection Act [COPPA] requires sites to obtain parental consent for the collection or use of any personal information from children under 13.)

Protecting Your Kids Online

Kids can get a lot out of the Internet, but not all communication or content is appropriate for young children or teens. To help ensure your kids’ online experiences are positive and safe, take an active interest in their online activities.

Read your child’s favorite blogs (short for web log), and visit and become a “friend” on your child’s social networking sites. Discuss what information is appropriate to share and what should be kept private. Explain that it’s not okay to go alone to see someone they “meet” on the Internet. Also let them know it’s not ok to share their passwords for social networking and other sites with friends. Accounts can be compromised and personal information stolen.

Keep the lines of communication open. Encourage children to share their questions and online experiences with you. Make

sure they understand that you will not punish them or take away Internet access if they let you know about any threatening or inappropriate communication, including bullying. And explain why it's wrong to bully others.

Report harassment and predatory behavior to the proper authorities, which may include school officials, local police, or the CyberTipline (www.cybertipline.com or 800-843-5678).

Discuss the various risks of Internet use, and set clear rules about what your kids can do and which sites they can visit online. Special software designed to manage Internet use can help you keep your children safer. Learn about family safety tools at kids.getnetwise.org/tools.

More Tips and Tools

Here are some additional ways to enhance your security and privacy online:

- **Back up** your files regularly (at least once per week).
- **Set your** operating system and other software to update automatically. You can choose to run updates at convenient times, when you are not using the computer.
- **Erase** your hard drive before selling, donating or disposing of your computer.
- **Make sure** a site is secure by looking for the SSL encryption ("https://" not just "http://") in the browser's address bar and a closed padlock or unbroken key in the browser window frame. Never enter debit or credit card information or bank account numbers unless you check this first. Most legitimate commercial websites have SSL encryption to make it safe to shop online.
- **When shopping online** it is safer to use a credit card than a debit card. The maximum liability for unauthorized charges on a credit card is \$50. Liability for unauthorized use on a debit card can be much higher, depending upon when you report the loss, and most debit cards are linked to your bank account, which means a thief could wipe you out.
- **Don't let** your web browser save sensitive IDs and passwords, like your bank account login or any site that stores your credit or debit card information for "one stop shopping." This is especially important at shared or public

computers. Clear this info by clicking on the "Tools" in most browsers and selecting "Delete Browsing History" or "Clear Private Data." (The words may be slightly different depending on the browser you use.)

- **Shop only** with online merchants you trust.
- **If you suspect** that an email message is a phishing attempt, contact the company directly. A legitimate business will never ask for your personal information in email. Delete the message and do not reply to the email.
- **Be careful** about opening attachments, visiting unfamiliar websites, and downloading "free" software. Don't download or share music or movie files with strangers—the file you receive could contain a virus, spyware or inappropriate content. (And, unauthorized file sharing of copyrighted material is illegal.)
- **Don't forward** "chain letters" and other email junk to other people, even if you think it's funny or informative. You could be seen as a spammer or, even worse, forward a destructive file to someone else. Check out all emails on anti-hoax sites (www.snopes.com or www.quatloos.com) before you hit the forward button so you don't spread "urban myths."
- **Trust your instincts.** If something appears too good to be true, it probably is. Your best defense online is good judgment.
- **Think twice** before clicking banner ads or pop-up windows. Click the X in the upper-right corner of the window to get rid of it.
- **Be aware** that free music, games and other downloads often include unwanted software in the download.
- **Don't use** email and instant messaging, or IM, to send sensitive personal information like credit card numbers, passwords, your date of birth or Social Security number.
- **Take similar precautions** if you connect to the Internet via a smart phone or other web-enabled device.

Assistance and Information

These organizations are good places to start if you want to learn more about Internet safety.

Family Online Safety Institute • www.fosi.org

The nonprofit Family Online Safety Institute works to make the Internet safer for children and their families.

OnGuard Online • www.onguardonline.gov

The U.S. federal government and the technology industry provide information and tips to promote online safety and security.

Privacy Rights Clearinghouse • www.privacyrights.org

The nonprofit Privacy Rights Clearinghouse offers a library of information, from tips for online job seekers to how to shop safely on the Internet.



Consumer Action, a nonprofit education and advocacy organization, offers news and information about privacy, including what your rights are and how to avoid scams.

Consumer Action

www.consumer-action.org

221 Main Street, Suite 480
San Francisco, CA 94105
415-777-9635 / TTY: 415-777-9456
hotline@consumer-action.org

523 W. Sixth Street, Suite 1105
Los Angeles, CA 90014
213-624-8327

Chinese, English and Spanish spoken

This publication was created by Consumer Action in partnership with Microsoft. © Consumer Action 2009

INTERNET SAFETY

A computer user's guide
to privacy and security

A Consumer Action Publication