

Minimize online risks by using the following steps

Protection software isn't perfect, so you should take additional precautions to reduce your vulnerability to online dangers. Here are the measures our experts consider most effective:

IMMEDIATE STEPS

1. Upgrade your operating system. If you use Windows XE enable the automatic Windows Update feature if you haven't already done so. Go to www.microsoft.com/protect and download and install Service Pack 2, which offers enhanced security. Consider upgrading to the next version of Windows when it comes out to get more security features. For earlier versions of Windows, run Windows Update from the Start menu.

The vast majority of viruses and spy-ware programs have targeted Windows-based PCs, which far outnumber Macintosh computers. So using a Mac can minimize your risk. Even so, keep your Mac up to date via the Software Update Control Panel. Also regularly update your Web browser and other major software, using the manufacturers' update instructions or features.

2. Use a firewall. Windows NP has a built-in firewall, so be sure to enable it. With older versions of Windows or with a Mac, install a software or hardware firewall, especially if you use a high-speed Internet connection. A software firewall costs \$30 to \$40. The firewall should provide both incoming and outgoing protection. If you have a home network, your router most likely has a built-in firewall. Change its default password and disable "remote administration" to prevent hackers from seizing control of the router.

3. Adjust browser security settings. If you use Internet Explorer 6, keep its security level at medium or higher to block Web sites from downloading programs without your authorization or automatically running Windows active scripts. Consider upgrading to Internet Explorer 7 when it becomes available, for stronger security features.

4. Consider an ISP or e-mail provider that offers security. AOL, Earthlink, MSN, and Yahoo offer spam filtering and virus scanning for e-mail at no extra charge for users. Use them as one layer of a multilayer defense. Check other ISPs' sites to find out what they provide.

5. Use antivirus software. You can obtain additional virus protection from ISPs, directly from a manufacturer's site, or at a retail store. Enable the auto-protect and automatic update features and keep your subscription current.

6. Use more than one antispysware program. None of the products we've tested catches every spyware variant. Using more than one program boosts your coverage, even if the second product is a free one. If you use more than one, you should enable the real-time protection for only one product. Download and install the free Microsoft AntiSpyware beta from www.microsoft.com/protect, but avoid free antispysware not listed in the Ratings. Keep your subscription to new spyware definitions current and regularly update the definitions or use the automatic update feature.

GOOD ONLINE PRACTICES

7. Regularly back up personal files. This safeguards your data in case of a security problem. Consider using a plug-in external hard drive as your main or backup storage, so that if the computer becomes disabled, you'll already have your files off the machine.

8. Be on the alert while browsing. Download only from online sources you trust. Be wary of ad-sponsored or "free" screen savers, games, videos, toolbars, music and movie file-sharing programs, and other purported giveaways; they probably include spyware that may damage your PC if it gets through your security. Children who share and download files should do so on a PC that doesn't contain confidential information or valuable data, such as financial records.

9. Avoid short passwords. To foil password-cracking software, use passwords that are at least eight characters long, including at least a numeral and a symbol such as #. Avoid common words, and never disclose a password online. With a broadband connection, shut off the computer or modem when you aren't using it. Don't post your e-mail address in its normal form on a publicly accessible Web page. Use a form, such as "Jane AT isp DOT com," that spammers' address-harvesting software can't easily read.

10. Use e-mail cautiously. Never open an attachment that you weren't expecting, even from someone you know. Never respond to e-mail asking for personal information. Forward fraudulent spam to the Anti-Phishing Working Group at reportphishing@antiphishing.org. Don't reply to spam or click on its "unsubscribe" link. That tells the sender that your e-mail address is valid.

11. Use multiple e-mail addresses. Use one e-mail address for family and friends, another for everyone else. You can get a free address from Hotmail, Yahoo, or 'a disposable-forwarding-address service such as SpamMotel. When an address attracts too much spam, drop it. Instead of an e-mail address like janedoe@isp.com, select one with embedded digits, like janesdoe2@isp.com. Report spam to your ISP to improve its filtering.

12. Take a stand. Don't buy anything promoted in a spam message. Even if the offer isn't a scam, you are helping to finance and encourage spam. If you receive spam that promotes a brand, complain to the company behind the brand.

13. Look for secure Web sites. With most browsers, to check whether a site is secure, look for an icon of an unbroken key or a lock that's closed, golden, or glowing. It will be in your browser's window (usually at the bottom), not within the Web page itself. Double-click on the lock to display the site's certificate, and be sure it matches the company you think you're connected to. Also make sure the site's address begins with "https:"

Information is from Consumer Report Magazine, September 2005. Visit ConsumerReports.org