## Consumer Reports WebWatch
## Cybercrime Prevention Project
## Fact Sheet #1: Ten General Tips to Stay Safe

This is the first in a series of ten consumer fact sheets in the Consumer Reports WebWatch "Look Before You Click" campaign, supported by a grant from the New York State Attorney General's office, to help educate New York consumers about Internet fraud.

If you have a computer at home, whether it's a laptop or desktop, you should follow these steps. Remember, a broadband (high-speed with no phone dialing) connection to the Internet is like another door into your house. Take the same kinds of security precautions with your broadband-connected home computers that you take when you leave your house.

1. Activate firewall protection. If your operating system (for instance, Microsoft Windows, either XP or Vista) has a firewall, spam blocker, or other built-in security application, make sure it's turned on – look in the lower right-hand corner of your Windows desktop for a security icon, and make sure you read pop-up warnings from your operating system on your security status. ZoneAlarm 7.0 is a free firewall for Windows XP.

2. Update and renew. Set your operating system and security software to update automatically. If you're using a PC, start the process at www.update.microsoft.com. Spam, spyware, and virus-detection programs incorporate "rules" or "definition" files that need to be current to catch the latest threats. When your software warns you to renew your service, be sure to do so, ensuring protection doesn't lapse. If you are having trouble downloading updates online, ask your operating system's publisher to send them to you on a CD-ROM.

3. Upgrade your operating system and browser. PC users should be running XP with service pack 2 at the least. Though Microsoft's newer Vista has some problems, it does let you surf in a protected environment that prevents online threats from damaging your operating system and contains an improved firewall. Consider using the Firefox browser, which has a pop-up blocker and will warn you if you come across a known phishing site. Later versions of Firefox will alert for badware.

4. Take advantage of security features offered by Internet service providers (ISPs) and others. The EarthLink Toolbar, for example, incorporates a scam and popup blocker, spyware scan, and home page protection. The Netcraft antiphishing toolbar warns about known phished sites. McAfee Site Advisor lets you know whether McAfee tested it and, if so, what it found, including viruses, spyware, spam, pop-ups, phishing, and consumer scams. It even overlays site reports on Web search results and automatically blocks access to sites that exploit browser weaknesses.

5. Shut off your computer when you're not using it. This can reduce the chance a malicious remote computer will penetrate your operating system security and access it. And you'll save energy. If you don't use your home computer consistently, however, make sure it's turned on for a period of a few hours, once a week, to allow security system and operating system updates to download and take effect on your machine.

6. Guard personal information. Never respond to e-mail requesting your passwords, user names, Social Security number, or other personal information, no matter how official it looks. If you're asked to call a telephone number, verify it independently.

7. Consider a Mac. Although Mac owners face the same problems with spam and phishing as Windows users, they have far less to fear from viruses and spyware. Because Apples are less prevalent than Windows-based machines, online criminals get less of a return on their investment when targeting Macs.

8. Watch what you download. The myriad of free utilities, games, and other software on the Internet can be useful, but many are laden with viruses and spyware. Try to download only from well-known manufacturers or trusted sites such as those at www.download.com, www.snapfiles.com, and www.tucows.com. If you are unsure, go to www.stopbadware.org, which now lists more than 250,000 suspect URLs.

9. Be sure you have antivirus software running. If you're having difficulty using the antivirus software that came with your machine, try Alwil's Avast!, free for home and non-commercial use at www.avast.com. If not Avast, make sure you run antivirus software and do regular scans.

10. Run two antispyware programs. Spyware is so insidious, and sometimes difficult to detect, that it warrants double protection. Set the better of the two programs to block spyware in real time. Use the other to scan whenever you suspect something might have escaped the first program. Try Spybot Search & Destroy, which is free, but consider making a donation.

For more information, and to keep up to date on ways to keep your home computers safe from unwanted invaders, bookmark Consumer Reports WebWatch.