SECURITY WATCH

Top Five Myths About Safe Surfing

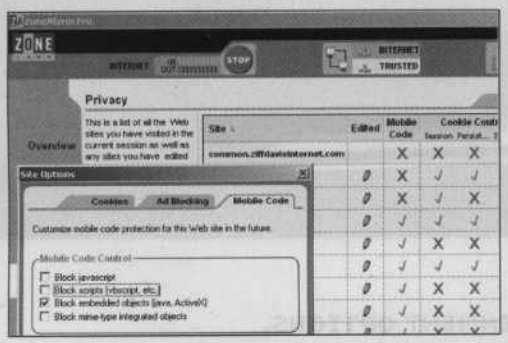
Don't let a false sense of security put you in danger.

By Leon Erlanger

Recently *PC Magazine* conducted a survey that asked participants to rate their broadband ISP services. We found out that many users don't completely understand the seriousness of potential threats or how to protect their PCs. The following are responses to the top five security misconceptions we encountered.

I don't keep important things on my PC, so I don't have to worry about security.

There was a time when this statement was partially true, but that time has long since passed. Current viruses, worms, and other threats, including the famous Love Bug, Nimda, and Blaster, spread blindly across the Internet to thousands or millions of PCs in a matter of hours, without regard for who owns them, what is stored there, or the value of the information they hold. The purpose of such attacks is nothing less than to wreak havoc. If you ignore the reality of these attacks, you are certain to be hit at one time or another. Even if your computer is not attacked directly, it can be used as a zombie to launch a denial-of-service or other attack on a network or to send spam or pornography to other PCs without being traced. Therefore, your civic responsibility is to protect your PC so that others are protected.



FIREWALLS can block inappropriate communication to or from your computer.

I can protect my PC if I disconnect from the Internet or turn it off when I'm not using it.

Wrong. If you connect to the Internet at all, you are a target. You could download a virus when you connect and not activate it until days later when you read your e-mail off-line. Even if you rarely connect to the Internet, you can get a virus from a file off of a network, floppy disk, or USB flash memory drive.

I can protect myself from viruses by not opening suspicious e-mail attachments.

Wrong again. The next virus you get may come from your best friend's or boss' computer if his e-mail address book was used to propagate an attack. Nimda and other hybrid worms can enter through the Web browser. And it is possible to activate some viruses simply by reading or previewing an e-mail. You simply must have a PC-based antivirus package.

I have a Macintosh (or a Linux-based system), not a Windows system, so I don't have to worry about being attacked.

It is true that most attacks target Microsoft Windows–based PCs, but there have been attacks against Mac OS and Linux systems as well. Some experts have predicted that the Mac virus problem will get worse, because Mac OS X uses a version of Unix. And although these systems have some useful security features, they can still be attacked.

My system came with an antivirus package, so I'm protected.

Not quite. First, if you haven't activated your antivirus package to scan incoming traffic automatically, you are not protected against e-mail and Web browser attacks. Second, new threats appear daily, so an antivirus package is only as good as its last update. Activate the auto-update features to stay on top of the latest threats. Third, an antivirus package can't protect you from every threat. In most cases you need a combination of solutions, including, at minimum, antivirus, a personal firewall such as Zone Labs' ZoneAlarm Pro, and a plan for keeping your operating system and software up to date with security patches. Antispyware and antispam utilities (such as PepiMK Software's SpyBot Search & Destroy and Norton AntiSpam 2004) will also help keep you safe.

Leon Erlanger is a freelance author and consultant.