New Computer? Six Steps to Safer Surfing

Washington Post, 12/18/04

To see the e-mail I get every day from readers about security issues is to develop a deep discomfort with the state of computing today. Keeping a Windows PC safe can demand a high degree of vigilance -- if cars needed the same constant care and feeding, the Beltway would revert to a country byway.

And yet all these attacks by viruses, worms, spyware and browser hijackers could have been prevented with some initial effort. It's completely feasible to put a computer on the Internet -- even one running Windows, the most attacked, least secure operating system around -- and never suffer a single successful attack.

Here's what to do to make that possible, starting -- as many people will this week -- when you take it out of the box and plug it in. Most of these steps apply only to Windows, but some pertain to Mac OS X (news - web sites) as well.

Step one is to barricade your Internet connection with a firewall. Without this, network worms such as Blaster can try to sneak onto your computer the instant it goes online, even if you don't run a single Internet program.

On any Windows XP (news - web sites) machine running Microsoft's Service Pack 2 update, a firewall should be on already. (If a new Windows computer doesn't have SP2, as evidenced by a Security Center control panel, take it back to the store -- there's no excuse for that not to be preinstalled.) On an older Windows machine, open the Network Connections control panel, right-click the icon for your connection, click the Advanced tab and click the checkbox under Internet Connection Firewall.

On a Mac, the built-in firewall must be switched on: Open the System Preferences window, select the Sharing category and then click the Firewall tab.

Step two is to download and install every security patch available. Don't do anything else online until the process concludes. In Windows, select Windows Update from the Start Menu's All Programs listing; in Mac OS X, select Software Update from the Apple-icon menu. Then set your computer to download future fixes automatically (you should need to do this only in pre-SP2 versions of Windows XP, where you'd open the System control panel and click the Automatic Updates tab).

The next three steps apply only to Windows; Mac users can skip ahead.

Step three is to activate and update the antivirus software on your computer. Most new PCs include only 90 days of updates, after which your protection will evaporate -- without a rap sheet on the latest viruses, your antivirus software can't identify them. Find out when your free coverage will end, then make a note in your calendar to renew your subscription before then. (If paying $20 or so for a year of virus protection bugs you, try repairing an infection.)

Step four is to update three core Internet programs, since older versions can suffer from security flaws. Get the latest versions of Microsoft's Windows Media Player (www.microsoft.com/windowsmedia/), RealNetworks' RealPlayer (www.real.com) and Sun Microsystems' Java software (www.java.com).

Step five is a big one: Download the free Mozilla Firefox Web browser (www.mozilla.org) and use that instead of Microsoft's Internet Explorer whenever possible. Firefox is not only simpler and more convenient than Internet Explorer, it's also much more secure -- since it's not hooked so tightly into Windows, it can't act as a transmission belt for viruses. And by not running Microsoft's ActiveX software, Firefox blocks a common route for spyware.

One thing you *don't* need to worry about on the Web -- contrary to what some security programs suggest -- is browser cookies. These small, inert text files are placed on your computer by most Web sites to customize your use of them; for example, The Post's site uses cookies to store registration info. These site-specific cookies are harmless.

Other, "third-party" cookies are set by ad networks to track ad viewership across multiple sites. They also pose no security threat. They do raise some privacy issues, but they can be easily blocked by any new browser without impeding your Web use. In either case, fretting over the nonexistent threat of cookies is a pointless distraction.

Step six is to use the most effective security mechanism ever invented, the human brain. In two words, be skeptical. Don't open unexpected e-mail attachments -- even if they come from a friend's e-mail address, since viruses scour infected PCs for e-mail addresses to impersonate. If you get an e-mail allegedly from your bank, ignore any links in it; log in by typing the bank's address into your browser yourself.

Most important, think twice about adding new, unknown software. What makes a program trustworthy? If a computer-savvy friend or a trusted publication says it's safe, that helps. If the program is available as "open source," meaning its programming code is free for anyone to inspect, that's another selling point.

If, after all these precautions, a malicious program does find its way onto your computer, Windows users can try using the System Restore utility to reset the computer to an older configuration (go to the Start Menu, select All Programs, then scroll up to the Accessories folder, then select its System Tools sub-folder). You can also limit the ability of other people to install software by giving them separate user accounts with limited access rights (select the Users system-preferences pane on a Mac, the User Accounts control panel on Windows).

But there is no replacement, on any computer, for common-sense caution, the same thing that keeps people safe in the face of far worse dangers in the real world.