Internet "spyware" emerges as new online threat

Reuters, 04.18.04, 8:43 AM ET

By Andy Sullivan

WASHINGTON, April 18 (Reuters) - Internet users have learned to keep an eye out for viruses, worms and "spam" e-mail.

Add another online hazard to the list: spyware.

Programs that hide in users' computers and secretly monitor their activities are emerging as the next high-tech plague, experts say.

Spyware can sap computing power, crash machines and bury users under a blizzard of unwanted ads. It can capture passwords, credit-card numbers and other sensitive data.

Spyware has even begun to burrow into popular culture.

"I was watching a soap opera the other day, and two characters were saying, 'Did you install that spyware in that person's machine?'" said Mozelle Thompson, a commissioner with the Federal Trade Commission.

On Monday, Thompson and other FTC officials will bring together policymakers, industry experts and consumer advocates to discuss the problem.

Educating consumers may be tricky because spyware is less visible than other online threats, experts say.

"Spam wants to be seen. Spyware doesn't want to be seen," said Dave Baker, vice president of law and public policy at Internet provider EarthLink Inc. (nasdaq: ELNK - news - people)

The first step is defining the problem. Some programs that have been labeled as spyware can be harmless, even helpful.

Many popular programs such as Kazaa and Morpheus that allow users to copy music and movies from each other's hard drives come bundled with applications that serve up pop-up ads or other marketing tools as a way to subsidize costs.

"Adware" programs like WhenU do not collect personal information from consumers, several peer-to-peer executives said, and users can easily remove them if they wish.

"The adware guys realize they're being lumped in as spyware, and I think they're cleaning up their act a lot," said Wayne Rosso, chief executive of Optisoft SL, which makes the Blubster file-sharing application.

CREATE A PROBLEM, OFFER A FIX

Other programs are clearly more malevolent. Some spyware has been known to disable a victim's computer and then advertise software to fix the problem.

Keystroke loggers, often distributed by e-mail viruses, allow identity thieves to capture bank-account numbers and other sensitive information.

An EarthLink scan of 1.1 million computers released last week turned up more than 300,000 malevolent programs.

The Center for Democracy and Technology on Friday proposed one way to separate the illegal from the merely annoying.

Software that "hijacks" Web traffic, tracks Internet users without their knowledge, or does not provide an easy way to be removed should be considered spyware, the nonprofit consumer group said in a draft letter also signed by high-tech firms and industry groups.

Legislatures have begun to turn their attention to the problem. Utah has already passed one law banning spyware.

WhenU, which would be prevented from serving its pop-up ads to Utah residents, has sued to block the law. Other tech companies say the Utah law is too broad and could inadvertently outlaw legitimate activities such as content filtering and technical support.

Two bills are pending in Congress to ban spyware, but observers say action is unlikely in this election year.

Lawmakers should consider broad online privacy protections against spyware and other online threats, said Ari Schwartz, an associate director at the Center for Democracy and Technology.

"If you keep trying to aim at the technology rather than the privacy issue, you're going to keep coming up with new issues to deal with every two years," Schwartz said.

Copyright 2004, Reuters News Service

List of some popular spyware/adware programs to avoid in the future

SpyWare and AdWare installed on your pc secretly gather your personal information and relay it to advertisers, thieves, or others via the internet, without your authorization or knowledge!! Many AdWare and SpyWare programs are made so they can't be removed from your PC through standard delete or uninstall methods!

How to Remove SurferBar

Bonzi Buddy Removal

Click2FindNow and I-Lookup Removal

Comet Cursor Removal

Date Manager Removal

Dubolom.com Homepage Hijacker Removal Instructions and Help NEW

FastSearch.cc Homepage Hijacker Removal Instructions and Help

Gator Software Removal

Hugesearch.net Homepage Hijacker Removal Instructions and Help

Search-Space.com and Start-Space.com Homepage Hijacker Removal Instructions and Help

How to Remove Global-Finder.com Homepage Hijacker

Globaltoolbar Removal

GoHip Software Removal

HotBar Toolbar Removal

Huntbar and Search Toolbar Info and Removal

Look2Me Removal Instructions and Help

Lookfor.cc (res://mshp.dll/index.html) Homepage Hijacker Removal Instructions and Help

MaximumSearch.net Homepage Hijacker Removal Instructions and Help NEW

Ncase Removal Instructions and Help

People OnPage Toolbar Info and Removal

Precision Time Removal

Prolivation.com Removal

SaveNow and NewDotNet Removal

SearchMyRequest.com Homepage Hijacker Removal Instructions and Help NEW

Smartsearch.ws Homepage Hijacker Removal Instructions and Help

How to Remove SpeedBlaster and MemoryMeter

WeatherBug Removal

Xupiter Removal

Xzoomy.com Removal

3 Network Defense

YOU MEET THE BIGGEST threat to your computer when you connect it to the Internet. Given the huge volume of well-crafted worms and infectious spam, it's a wonder more computers haven't turned into zombies obeying the commands of malicious hackers. Here's how to prevent your PC from joining the digital undead.

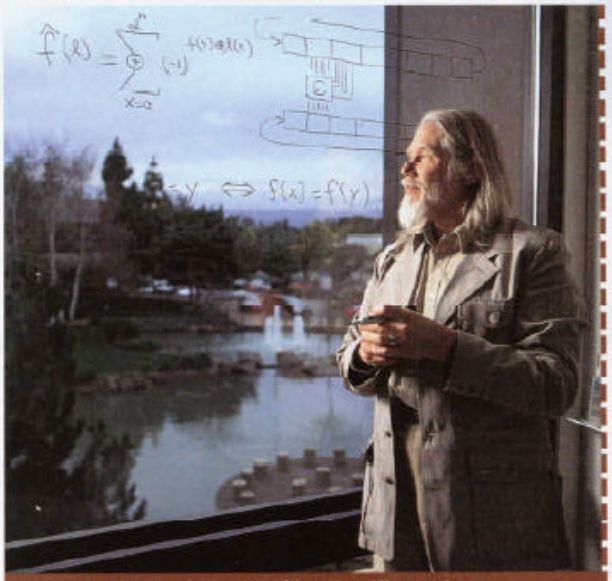
Put a firewall on every PC: Regardless of its connection type—dial-up, broadband, or wireless—any computer that connects to the Internet needs a firewall to protect it from attacks over the network and rogue programs sending data out. In fact, your best bet is to use two firewalls: an external, hardware firewall, such as the kind built into most wired and wireless routers (and some cable or DSL modems); and a software firewall that runs on your PC, watching your applications.

In addition to blocking unsolicited incoming and outgoing traffic, hardware firewalls provide Network Address Translation. NAT, in combination with the router's built in Dynamic Host Control Protocol (DHCP) server, masks your true IP address from computers outside your local network, making your PC nearly impossible to target. Because hardware firewalls are the first line of defense against incoming attacks, properly configuring them in accordance with the manufacturer's documentation is crucial. In particular, you have to create a strong administrator password to prevent someone from taking control of your firewall.

Software firewalls protect you from inside threats—viruses, Trojan horses, and spyware—that may come to reside on your PC. For more details on both types of firewalls, including a list of four free software firewalls, see the December 2003 *Internet Tips* column (find.pcworld.com/40901).

Spurn spyware: If new programs unexpectedly show up in your taskbar or browser toolbar, you've probably been stung by some form of adware or spyware. To avoid spyware, watch out for unwanted components while installing freebies, and use free anti-spyware utilities like PepiMK Software's Spybot Search & Destroy (find.pcworld.com/28403) and Lavasoft's Ad-aware (find.pcworld.com/37322). Commercial keylogging software—spyware installed on your PC by a boss, spouse, or other snoop when you're not around—is harder to detect and remove. See this month's *Internet Tips*, page 160, for advice on tracking it down and removing it.

Boost wireless network security: Wireless networks are a wonderful innovation, but they're also a security nightmare because they have no boundaries. Anybody who lives, walks, or drives within radio range of your wireless hub can probably hitchhike on your wireless ▶



Whitfield Diffie, Chief Security Officer, Sun Microsystems

"To protect yourself fully, the right thing to do is to replace Windows with a Unix-like operating system, like Linux, Mac OS, or Solaris."

Print

Protect Your PC: Print All Three Steps

Operating System: Windows Me
Last Updated: September 9, 2003

To print these instructions, click the **Print** button in the upper right of this window. When you are done, close the window to return to the previous page.

Step 1: Use an Internet Firewall

Before you connect your computer to the Internet, you should install a firewall. This is a piece of software or hardware that helps prevent hackers, and many types of viruses and worms, from accessing your computer.

Firewalls are the most important first line of defense for computer security. You should also use Windows® Update and antivirus software to help protect your PC.

If you have a computer with Windows 2000 Professional, Windows Millennium Edition (Me), Windows 98, Windows 95, or Windows NT, you should get and install either a hardware or software firewall. The following resources provide more information about some firewall options.

Hardware Firewalls

Hardware firewalls are a good alternative for earlier versions of Windows. Many wireless access points and broadband routers for home networking have built-in hardware firewalls. These provide sound protection for most home networks. The Microsoft Broadband Networking Wireless Base Station is one example of a wireless access point with a built-in hardware firewall and other integrated home networking features.

Software Firewalls

Software firewalls are available from several vendors, including:

- BlackICE PC Protection
- Computer Associates (12 months free)
- McAfee Security
- Symantec
- Tiny Software: Tiny Personal Firewall
- ZoneAlarm

To learn more about firewalls, read Checklist: Install a Firewall, from the Microsoft Security Web site. This article includes a discussion of software firewalls made by other companies, as well as hardware firewalls and network routers. This information can help you select a firewall solution if you use an earlier version of Windows on your computer.

If you have a different configuration, a small network, or if you encounter issues with regards to your firewall, see the Frequently Asked Questions about Firewalls.

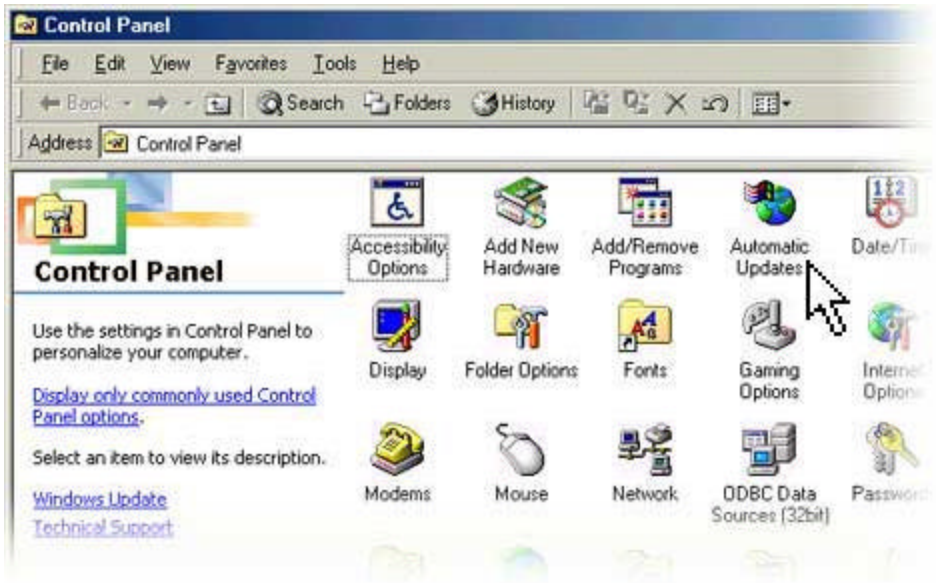
Step 2: Get Computer Updates

If you are using Microsoft® Windows Me, you can take advantage of Automatic Updates, which can automatically download the latest Microsoft security updates while your computer is on and connected to the Internet. (If you are not sure what version of Windows you are using, you can find out by following the instructions for checking your operating system version).

To use Automatic Updates to download and install any future critical security updates from Microsoft:

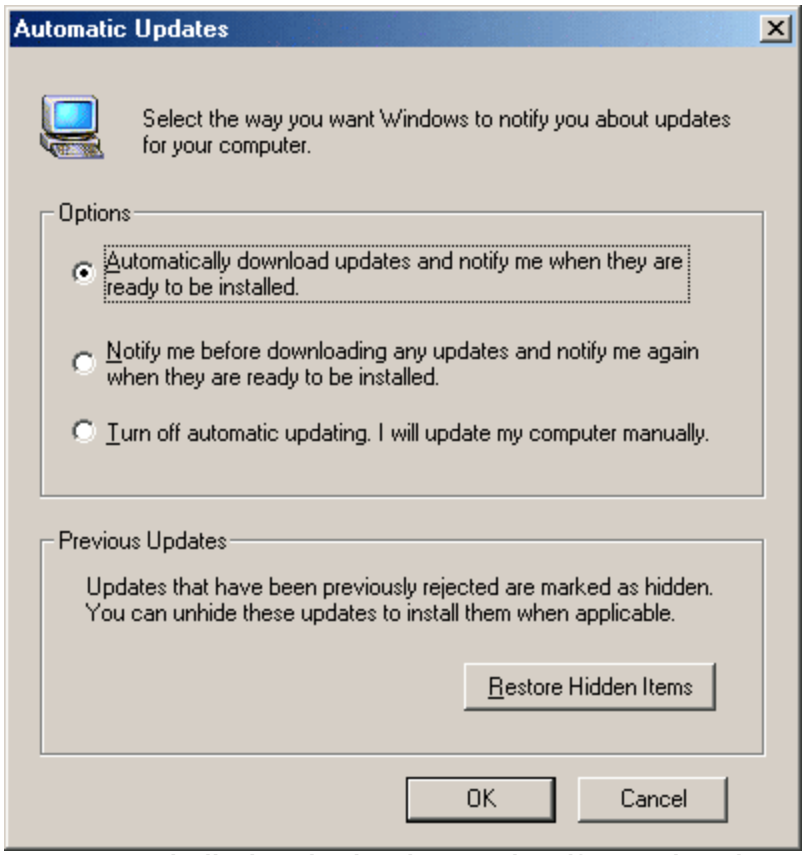
1. Click **Start**, and then click **Control Panel**.
2. Click **Automatic Updates**.

   If you don't see the **Automatic Updates icon**, click **view all Control Panel options** on the upper left of the window.



Click **Automatic Updates**

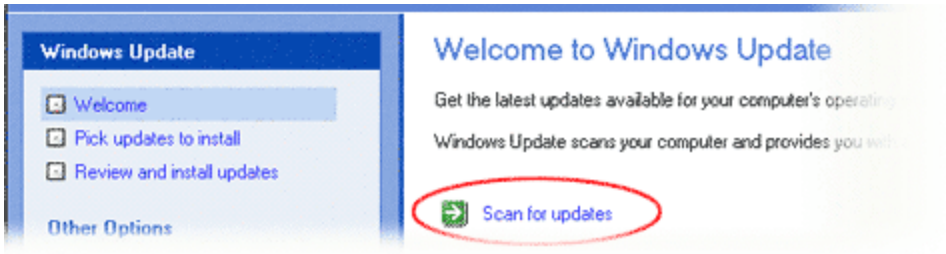
3. Choose an Automatic Updates setting. We recommend automatically downloading the updates. Follow the rest of the steps to complete setting up **Automatic Updates**.



Click **Automatically download updates and notify me when they are ready to be installed**

You will now download all future updates automatically. If you haven't used Automatic Updates in the past, you may have missed some updates, however. Here's how you can bring your computer up to date:

1. Go to the Windows Update Web site at http://windowsupdate.microsoft.com.
2. On the Windows Update site, click **Scan for Updates**. Windows Update will scan your computer and give you a pre-selected list of critical updates.

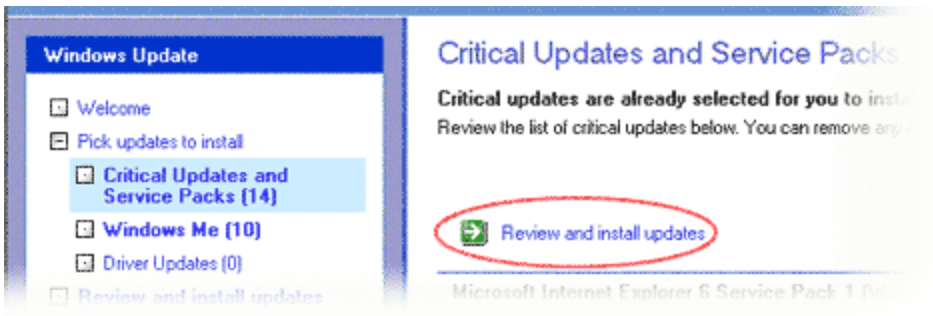


Click **Scan for updates**

Note: Slower modems may take several hours to download all recommended updates the first time you use Windows Update. Your download times will vary depending on how long it has been since you last updated and your modem speed. To reduce download times, run Windows Update when you will not be

using your computer for other Internet-related tasks.

3. In the **Pick updates to install** list on the left side of your screen, click **Critical Updates and Service Packs.** Windows Update will create a list of the updates appropriate for your computer.
4. Click **Review and install updates**. Select the updates to install, then click **Install Now** You may need to restart your computer after installing the updates.



Click **Review and install updates**

Note: Be sure to go back to Windows Update after rebooting to check for any additional downloads. You may need to do this several times.

Important note for Microsoft Office users. You should also visit the Office Update site to install the latest security releases.

Step 3: Use Up-to-Date Antivirus Software

Antivirus software is a program that either comes installed on your computer or that you purchase and install yourself. It helps protect your computer against most viruses, worms, Trojans, and other unwanted invaders that can make your computer "sick." Viruses, worms, and the like often perform malicious acts, such as deleting files, accessing personal data, or using your computer to attack other computers.

Help your computer stay healthy by asking yourself the following questions:

1. **Do you have antivirus software installed on your computer?**

   Many major computer manufacturers include at least a trial version of a popular antivirus package on new computers.
   - Click **Start**, and then click **Programs**. Look for an item in the list with a name like McAfee, Norton, or Symantec.
   - If you don't have antivirus software installed, check out the following antivirus software companies for special offers on their products:
     - Computer Associates (12 months free)
     - McAfee Security
     - Symantec
   - If you already have antivirus software installed, but you want to install a new product from a different company, be certain to uninstall your current product before installing the new one. Leaving the previous version installed can cause conflicts on your system.

2. **Is your antivirus software up to date?**

   Out-of-date antivirus software means ineffective antivirus software. Antivirus software relies on regular updates to help protect against the latest threats. If you aren't subscribing to these updates, your computer may be vulnerable to threats.
   - Make sure you have activated a subscription for continuous updates of your antivirus software.
   - Most antivirus software updates itself when you are connected to the Internet. To ensure your software is up to date, open your antivirus program from the **Start** menu or the taskbar notification area and look for update status. If you still aren't sure if your antivirus software is up to date, contact your antivirus software provider.
3. **Is your antivirus software set up correctly to provide the best protection possible?**

   The following settings should be turned on by default when you install the software. If you turn them off for any reason, be sure to turn them back on before you connect to the Internet.
   1. **"On-access" or "real-time" scanning** should be turned on. An icon in your notification area should appear to indicate that this setting is enabled.
   2. Antivirus software should perform a **scheduled scan of your hard disk.**
   3. Antivirus software should be configured to **scan e-mail messages**.