

## 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](#) 

[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](#) 

[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](#) 

[Smartsearch.ws Homepage Hijacker Removal Instructions and Help](#)

[How to Remove SpeedBlaster and MemoryMeter](#)

[WeatherBug Removal](#)

[Xupiter Removal](#)

[Xzoomy.com Removal](#)

PC SECURITY

# 3 Network Defense



**Y**OU 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

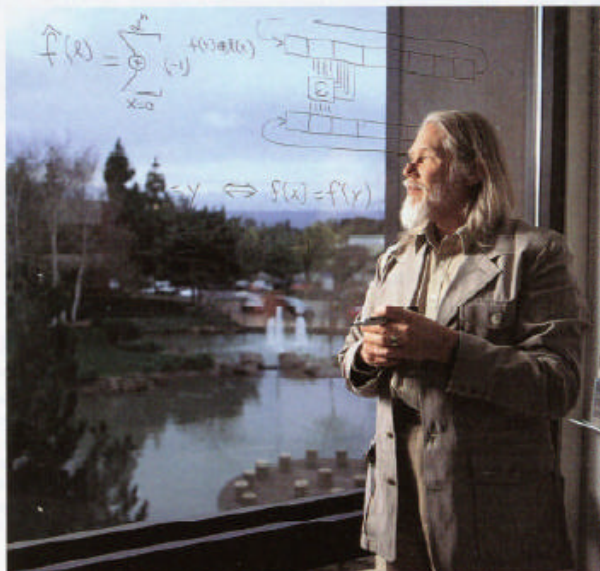
administrator password to prevent someone from taking control of your firewall.

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](http://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 util-

ities like PepiMK Software's Spybot Search & Destroy ([find.pcworld.com/28403](http://find.pcworld.com/28403)) and Lavasoft's Ad-aware ([find.pcworld.com/37322](http://find.pcworld.com/37322)). Commercial key-logging 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 - Windows XP

## Print All Instructions

Operating System: Windows XP  
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

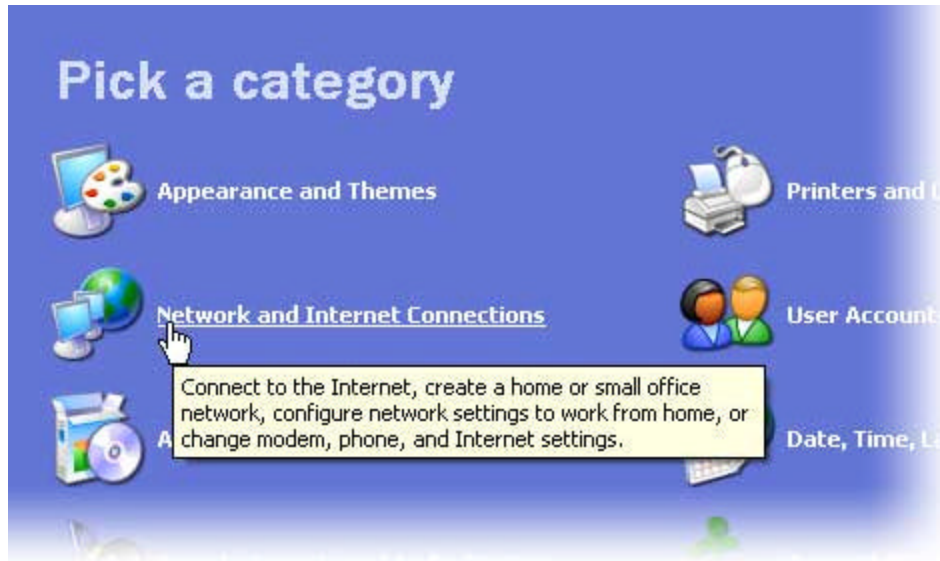
Before you connect your computer to the Internet, you should install a firewall. This is a piece of software or hardware that helps protect your PC against hackers and many computer viruses and worms. If you have the Microsoft Windows® XP operating system, you can use its built-in Internet Connection Firewall. Using a firewall is the most important first line of defense for computer security. You should also use Windows Update and antivirus software to help protect your PC.

**Important** Internet Connection Firewall works by blocking certain types of potentially harmful network communication. However, it also blocks some useful network communication tasks (for example, sharing files or printers through a network, transferring files in applications such as instant messaging, or hosting multiplayer games). We highly recommend that you use a firewall because it helps protect your computer today. If you choose to turn on Internet Connection Firewall you can come back later for help with unblocking useful network communication tasks. For more information, please refer to the [Frequently Asked Questions About Firewalls](#).

The steps below tell you how to make sure the Windows XP firewall is turned on. If you have a different configuration, a home network, a different version of Windows, or if you encounter problems during the steps, see the [Frequently Asked Questions about Firewalls](#).

#### To turn on the Internet Connection Firewall

1. Click **Start**, and then click **Control Panel**
2. Click **Network and Internet Connections**, and then click **Network Connections**.



Click **Network and Internet Connections**



Click **Network Connections**

**Note:** If the **Network and Internet Connections** category is not visible, click **Switch to Category View** on the upper left of the window.



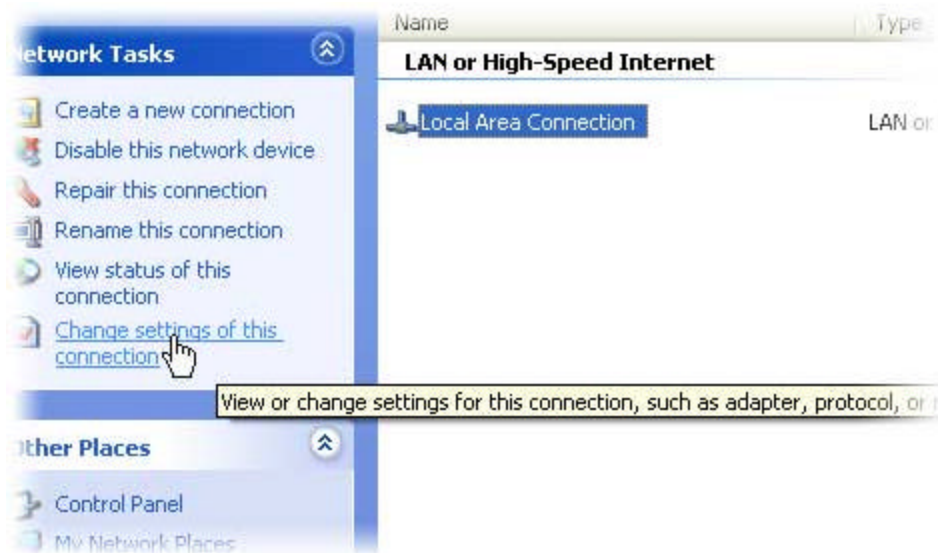
Switch to Category View

3. Under the **Dial-Up** or **LAN or High Speed Internet** heading, click the icon to select the connection that you want to help protect.



Select a connection

- In the task pane on the left, under **Network Tasks**, click **Change settings of this connection**. (As a shortcut, you can right-click the connection you want to help protect, and then click **Properties**.)



Change connection settings



Alternatively, right-click the connection, and click **Properties**

5. On the **Advanced** tab, under **Internet Connection Firewall**, check the box next to **Protect my computer and network by limiting or preventing access to this computer from the Internet**.



Check the box to protect your computer and network

After you check the box and close the **Properties** window, the firewall is turned on. The firewall may interfere with some network operations such as file and print sharing, networking-related programs, or online games. For more information about fixing these issues, see the [Frequently Asked Questions](#) page listed below.

If you have more than one computer, want more technical information, or just want to learn more about Internet firewalls, see the [Frequently Asked Questions About Firewalls](#) page.

## Step 2: Get Computer Updates

The Microsoft Windows® XP operating system includes the Automatic Updates feature, 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](#)).

Before you turn on Automatic Updates, it's a good idea to bring your hardware and software up-to-date using Windows Update. Here's how:

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

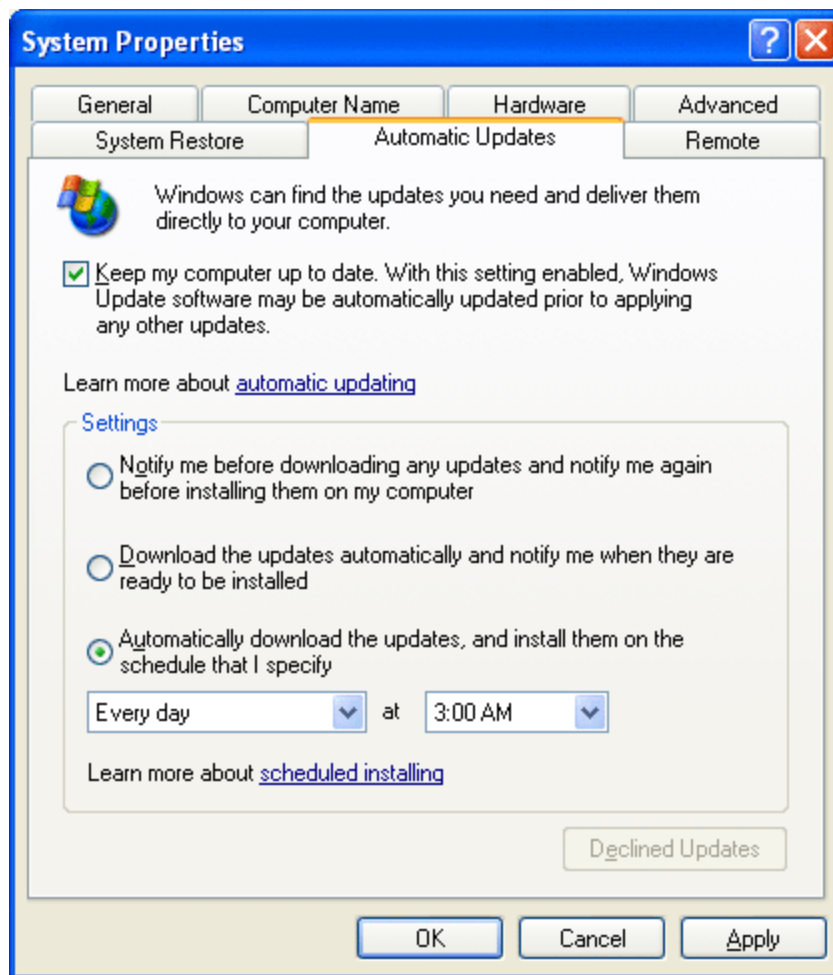
1. Click **Start**, and then click **Control Panel**.

2. Click **Performance and Maintenance**.

If the **Performance and Maintenance** category isn't visible, click **Switch to Category View** on the upper left of the window.

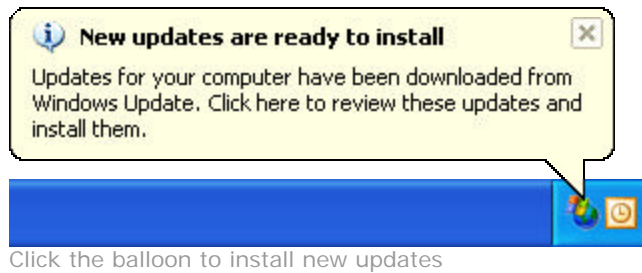
3. Click **System** to open the **System Properties** dialog box. You'll see a screen like the one below.
4. On the **Automatic Updates** tab, check the box next to **Keep my computer up to date**.
5. Choose a setting. We strongly recommend choosing **Automatically download the updates, and install them on the schedule that I specify**.
6. If you choose the option to automatically download and install updates, select a day and time when your computer will be turned on, so the installation process can be finished.

**Note:** We recommend a daily update.



Choose **Automatically download the updates and install them on a schedule that I specify**

If you set up Automatic Updates to notify you, or if your machine was off at the scheduled installation time, you will see a notification balloon like the one below. Click the notification balloon to review and install the updates.



## Using Windows Update

Here's how you can bring your computer up to date now. You can also use these instructions to keep up with the latest non-critical updates:

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, including service packs.



**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. (Critical updates will be selected for download automatically.)

4. Click **Review and install updates**. Select the updates to install, including any service packs and the critical updates pre-selected for you, and 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 updates. 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

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.

- o Click **Start**, and then click **Programs**. Look for an item in the list with the word "antivirus" in it, or for McAfee, Norton, or Symantec, which are manufacturers of popular antivirus products.
- o 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](#)
- o 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.

- o Make sure you have activated a subscription for continuous updates of your antivirus software.
- o 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.

- o **"On-access" or "real-time" scanning** should be turned on. Most antivirus products include an icon that appears in the notification area at the lower right of your screen to indicate that this setting is enabled.
- o Antivirus software should perform a **scheduled scan of your hard disk**.
- o Antivirus software should be configured to **scan e-mail messages**.