10 things you should know about fighting spyware in Windows XP

Version 1.0
February 3, 2006

By Greg Shultz

Today's cybercriminals are a crafty bunch, and they've mastered the art of infiltrating your computer and populating it with spyware—a broad category of malicious software programs installed on your computer without your knowledge or permission. Spyware is designed to operate in the background to perform such dubious tasks as gathering information about your computer usage and reporting back to a central database or diverting control of your computer to operations that benefit a cybercriminal's goals. Regardless of the nature of the spyware, it is definitely in your best interest to get rid of it as fast as you can. Here are 10 things you should know about fighting spyware in Windows XP.

1 Identify the presence of spyware

Since spyware is designed to infiltrate your computer and clandestinely run in the background, how do you know when it is present? Even though spyware does its best to be sneaky, you can look for several telltale signs to identify the existence of spyware on your computer:

- Mysterious abundance of pop-up advertisements
- Internet Explorer's home and search pages suddenly change
- Internet Explorer contains uninvited components, such as toolbars
- Unknown icons appear on desktop, system tray, or toolbars
- Computer boots slower, runs sluggish, or unexplainably crashes

2 Keep your operating system and software up to date

All kinds of malicious applications are designed to seek out and take advantage of vulnerabilities in your operating system and software. So one important key to keeping spyware at bay is to proactively keep your Windows operating system and Microsoft software as up to date as possible:

- Upgrade Windows XP with SP2. (Learn more on the Windows XP Service Pack 2 site.)
- Make sure that the Automatic Updates feature is enabled in Windows XP SP2's Security Center.
- Switch from Windows Update to Microsoft Update. (Connect to the Windows Update site and click the Upgrade To Microsoft Update link).

3 Use a firewall

A firewall can be either hardware or software that monitors your Internet connection and blocks unsolicited requests to gain access to your system. Even if you have a hardware firewall on your network, you should run a software firewall on your computer. Doubling your protection never hurts.

If you're running Windows XP SP2, the Windows Firewall is turned on by default. However, you can install and use any third-party firewall software you want. To learn more about using and configuring the Windows XP SP2 Windows Firewall, read the Microsoft article "Understanding Windows Firewall."

4 Scan your system with an anti-spyware program

You should regularly use an anti-spyware program, which will to scan for and remove spyware from your computer. Although a number of commercial anti-spyware scanning programs are available, you'll also find several good anti-spyware programs that are free to download and use:

- Spybot Search & Destroy
- Ad-Aware SE Personal Edition from Lavasoft
- Microsoft Windows AntiSpyware beta

5 Know spyware when you see it

After using an anti-spyware program to scan your system, you may end up viewing a report with huge list of items reported as spyware. Some items are obviously spyware, such as something called ClickWatch, but other items might not be so easy to identify. Then you're left trying to decide whether to remove the item or leave it alone. When you're in doubt, here are a few ways to seek answers:

- Check you anti-spyware vendor's site; they often keep a database of spyware offenders and detailed information.
- Check the Spyware Guide site.
- Check Computer Associate's Spyware Encyclopedia.
- Just Google the name of the item and see what turns up.

6 Use a real-time anti-spyware scanner

If you can't seem to avoid spyware sources or your computer is used by young surfers who may not understand the threat posed by spyware, you should consider using an anti-spyware program with a real-time monitoring component that runs in the background, looking for and blocking spyware as you surf the Internet. For example, Spybot Search & Destroy provides a real-time monitoring component called TeaTimer. The free version of Ad-Aware doesn't contain a real-time monitoring component—you have to purchase one of the Ad-Aware versions that contains the Ad-Watch real-time monitoring component.

7 Keep Internet Explorer's Internet zone set to Medium

Spyware primarily infiltrates your system via Web sites containing hidden traps that ambush your computer before you have a chance to figure out what's going on. To protect your computer from such unauthorized access, Internet Explorer provides a range of Security settings that control how much information you'll automatically accept from a Web site. When you install SP2, the setup procedure sets the Internet zone to Medium, which is the recommended level. A Medium security setting offers just enough access to make Web browsing enjoyable, yet safe.

It's easy to change the Security settings, and someone may inadvertently (or intentionally) lower the level, thus opening the door to spyware. As a result, it's a good idea to keep tabs on Internet Explorer's Security settings for the Internet zone:

1. From within Internet Explorer, pull down the Tools menu and select Internet Options.
2. In the Internet Options dialog box, choose the Security tab.
3. Select the Internet zone and check the Security level setting.
4. If it's not set to Medium, click the Default Level button.

For more information on Internet Explorer's Security settings, see the Microsoft article "Working with Internet Explorer 6 Security Settings."

8 Use Microsoft's online Malicious Software Removal Tool

If you suspect that your system has been compromised by some form of spyware, chances are good that other malicious software snuck in at the same time. In that case, you may want to use Microsoft's online Malicious Software Removal Tool to check for other anomalies. (Microsoft updates this tool with new signatures on the second Tuesday of each month.)

1. Use Internet Explorer to connect to the Malicious Software Removal Tool page.
2. In the Scan And Clean Your PC panel, click the Check My PC For Infection button.
3. When you see the Microsoft End-User License Agreement dialog box, select the I Agree option and click Continue.
4. If Internet Explorer prompts you to install the ActiveX control, allow the installation and then click the Check My PC For Infection button again.
5. When prompted to install the Malicious Software Removal Tool, click the Install button.
6. When the scan is a complete, review the report displayed on the page.

9 Use the Pop-Up Blocker

Pop-up windows containing innocuous advertisements or goofy messages are often the calling card of some devious spyware program. By default, SP2 installs and enables Internet Explorer's Pop-up Blocker with the default Filter level setting of Medium. However, this setting will often block legitimate pop-ups that users need to see. As a result, many people decide that the inconvenience is more annoying than the potential risk and turn off Pop-up Blocker. It's easy to do: Tools | Pop-up Blocker | Turn Off Pop-up Blocker.

However, the ability to display a pop-up is often all the spyware needs to infiltrate a system. So instead of turning off the Pop-up Blocker, you should use the Exceptions feature to allow pop-ups from those Web sites you trust:

1. Choose Tools | Pop-up Blocker | Pop-up Blocker Settings.
2. Type the address of the Web site in the appropriate text box and click the Add button.
3. Make sure that the Filter level setting is set to Medium.
4. Click the Close button.

10 Close pop-ups properly

If you do happen to encounter a pop-up window, don't click any button inside the window no matter what it says. A lot of spyware will try to trick you into allowing it into your system by prompting you to click an innocent-looking OK or Cancel button in a window designed to look like a dialog box. Never do that! Always use the red Close button in the upper-right corner of the window.

Greg Shultz has been using PCs since 1986, when he acquired a Kaypro 16 "luggable" running MS-DOS 2.11 and began programming in Microsoft BASIC and Turbo Pascal. He began his career in the publishing industry as a technical editor for PCM magazine, a publication focused on Tandy computers. He later became a technical journal writer, specializing in the Windows operating system, at The Cobb Group (which later became ZD Journals and then Element K Journals). Greg is now a freelance technical writer who regularly writes articles for ZDNet and TechProGuild. You can visit his Web site at www.TheWinWiz.com.

Additional resources

- TechRepublic's **Downloads RSS Feed** XML
- Sign up for our Downloads Weekly Update newsletter
- Sign up for our Network Security NetNote
- Check out all of TechRepublic's free newsletters
- "The Anatomy of Spyware" (TechRepublic download)
- "Resource list: Anti-spyware tools" (TechRepublic download)
- "10+ things you should know about troubleshooting a slow PC" (TechRepublic download)

Version history

Version: 1.0
Published: February 3, 2006

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team