

# TCS General Meeting

## November 30, 2004

### Spyware



<http://www.pcmag.com/article2/0,1759,1618797,00.asp>

#### **Antispyware**

August 3, 2004

By John Clyman

Adware and spyware are a growing nuisance and threat. They hijack your browser, pop up undesired ads, redirect you to unsavory sites, and even monitor your behavior for potentially malicious purposes. So it's no surprise that antispyware utilities are becoming essential components of desktop security arsenals. Though no antispyware utility provides an impenetrable defense, the following tips can help you get the most out of them.

We have one piece of general advice: When you install a new application, read the end user license agreement (EULA) carefully. We know it's boring. But shareware and freeware often pack a spyware payload, which should appear in the EULA. Don't click on that Agree button without understanding exactly what you're agreeing to.

**Install and configure the software.** Installing most antispyware programs is straightforward, but some won't download their newest spyware detection signature files until you manually instruct them to. Make that your first task, then set the software to download updates automatically, if it gives you that option.

It's also a good idea to turn on any real-time monitoring and blocking the program offers. But don't consider that a panacea; we've found that real-time monitors don't always detect spyware before it finds its way onto your machine. If you drill into the configuration options of many antispyware products, you'll find dozens of detailed settings that you can tweak to your liking. We recommend that you start with the default settings and explore other options as you learn more about spyware.

**Run full scans regularly.** Set your antispyware software to scan on a scheduled basis—at least once a week—and every time the system boots, if these options are available.

**Understand scan results.** Antispyware software works by trying to detect distinctive signs that spyware places on your system. These spyware traces consist of running processes, Registry entries, files (including shortcuts placed in your Start menu or on your desktop), and tracking cookies.

Running processes indicate that suspected spyware is active in memory. Registry entries and files are signs that spyware is or has been resident on your hard drive. Although antispyware utilities often display details of exactly which processes, Registry entries, and files appear

suspect, you can usually gloss over the detailed trace list and just look for names of suspected spyware.

Tracking cookies are a special case. By themselves, cookies are benign snippets of data. But because they can be tied to an individual IP address, they can be used to track a user's activity over multiple Web sites, representing a potential privacy risk.

**Review the threats and take action.** Deciding what to do about spyware can take some thought. Unlike viruses and worms, which you absolutely don't want on your system, there may be cases where you're willing to accept certain types of spyware or adware. Some programs, utilities, games, and browser add-ons may include adware or spyware and will break if you remove these components.

If you deem the benefit sufficient and the nuisance or threat insignificant enough, you might be willing to accept that trade-off. (Most antispyware tools will let you restore a removed item if the program it rode in on no longer works after the spyware removal.)

So how can you get the information you need to make that judgment call? Ideally, your antispyware utility will present informative explanations of the nature and severity of the threat posed by the spyware it detects. You can also search the Web for the application name and visit spyware information sites like Spyware-Guide.com and PestPatrol's Center for Pest Research ( [www.pestpatrol.com/pestinfo](http://www.pestpatrol.com/pestinfo) ).

After you remove spyware, scan again. Spyware can be surprisingly resilient. After you've scanned and eliminated spyware, reboot your machine and scan once again immediately. You may find that some of the spyware has reinstalled itself and needs to be removed anew.

Double up for safety: Use a second antispyware tool. No antispyware tool is foolproof, and often a second one will find something the first missed.

If repeating the cycle again with a second utility doesn't solve the problem, search the Web for further help; removing some particularly sticky spyware may require specialized tools. You can also try an online-only free scan like Spy Audit, from Webroot ( [www.webroot.com](http://www.webroot.com) ), or Pest Scan, from PestPatrol ( [www.pestpatrol.com](http://www.pestpatrol.com) ). As a last resort, you might try following instructions for manual removal, but be sure to back up any affected files or Registry keys first.

Respond to real-time alerts. If you're using antispyware software with real-time monitoring and blocking, you'll eventually get an alert that new spyware has been detected on the system. If these alerts occur when you're in the middle of a software installation process, try to learn about potential threats from the application before you elect to complete the installation.

### **Recommended Products**

Spybot Search & Destroy  
Webroot Spy Sweeper

[End of PCMag Article]

---

# Tools, patience needed to fight spyware

By MICHAEL HIMOWITZ Los Angeles Times-Washington Post News Service  
8/10/2004

[http://www.tulsaworld.com/NewsStory.asp?ID=040810\\_Sy\\_E6\\_Tools6541](http://www.tulsaworld.com/NewsStory.asp?ID=040810_Sy_E6_Tools6541)

Tired of spyware, adware and other slimeware that sneaks onto your computer, snoops while you surf the Web, steals personal information, hijacks your Web browser and slows your PC to a crawl? You don't have to put up with it.

With a basic toolkit and a lot of patience, you can get rid of most of these parasites and maybe keep them from coming back.

Before you start, look for help online. Spyware is so pervasive and annoying that a whole cottage industry of Web sites has grown up to help keep it in check. I'll be mentioning a lot of these resources here -- you'll find direct links to all of them (and more that I didn't have room to mention) at [www.baltimoresun.com/spyware/](http://www.baltimoresun.com/spyware/).

That said, the best rule for fighting spyware is to keep out of harm's way. Here's how:

- Keep your operating system updated. Microsoft releases security updates at least once a month. Surf to [windowsupdate.microsoft.com](http://windowsupdate.microsoft.com) and download all updates labeled "Critical."
- Steer clear of known sources of adware and spyware. File-sharing programs such as Kazaa, Grokster, Lime Wire and BearShare are advertising-supported. They make their money by installing adware on your machine and charging advertisers to track your Web browsing and pop up targeted ads.
- Save yourself grief by keeping them off your computer in the first place. If your kids insist, you can also look for spyware-free versions of file-sharing software that tap into the same file-sharing networks, such as Shareaza, Gnucleus, XoloXcq and Bearshare Lite. They're on a variety of download sites. Just realize that spyware can sneak in from the files the kids download, too.
- Don't accept offers to download file-viewers, toolbars, cursor tools, form fillers or other programs that are supposed to enhance your Web-browsing experience. These are common on gaming and porn sites, but can crop up anywhere. With the exception of Adobe, Macromedia, Quicktime and a few other well-known add-ons, these are likely to be spyware traps. In fact, when one of these windows pops up, don't click on the decline button. Close the popup window by clicking on the "X" in the upper right corner.
- As a corollary, never click anywhere inside a popup ad window -- especially one that says your computer is infected and offers anti-spyware software. Clicking is often enough to download a nasty bug. Use the "X" in the upper right-hand corner to close the window. If there's no "X" in sight (a common tactic), hit ALT-F4 to close the window. And if that doesn't work, hit CTRL-ALT-DEL to bring up the Windows task manager and end your Internet Explorer session.
- Install a popup ad stopper, which eliminates many opportunities to download spyware in the first place. Two with excellent pedigrees are included in the Google and Microsoft toolbars (exceptions to the no-toolbar rule). For links to others, as well as a nifty test of your own popup-stopper, visit [www.popuptest.com](http://www.popuptest.com).
- Disable Windows Messenger. This shouldn't be confused with Microsoft's instant messaging program. It's an internal communications program used by system administrators and exploited

by popup ad pushers. The quickest way to disable it is to download a program called ShootTheMessenger from Gibson Research.

- Increase Internet Explorer's security settings. Click on Tools/Internet Options and select the Security tab. Click on the Internet Zone, then Custom Level. This displays an options list. In the section marked ActiveX, set Download signed ActiveX Controls to Prompt. Set Download unsigned ActiveX controls to Disable, and set Initialize and Script ActiveX Controls not marked as safe to Disable.
- Consider switching to another Web browser, except when you're visiting a handful of sites that absolutely require Internet Explorer, or IE, to function properly. Mozilla, Netscape and Opera are three good browsers that have far fewer security flaws than IE and won't conflict with it. You can download them free online.
- Install a spyware blocker. Most spyware removers include software that tries to "inoculate" your computer against new threats by monitoring programs that install Browser Helper Objects, or BHOs, download ActiveX Controls, or make specific changes in your Windows registry. If you use one of these programs, you should turn this protection on.

Although it won't remove existing spyware, one of the best standalone blockers is Javacool's free SpywareBlaster, or its more aggressive cousin, SpywareGuard.

Even with the best tools, removing spyware can be a long and frustrating process -- particularly if your machine has multiple infections or you're running Windows XP with multiple users. Earthlink, the nationwide ISP, surveyed a million of its customers' PCs and found an average of 29 spyware components on each one.

Professional troubleshooter Marc Seidler of computerdoctors.net, my guru in these matters, says he sees 350 to 400 discrete spyware components on most of the computers he's called in to disinfect. This is one reason why no single spyware remover will nab them all.

[End of Tools document]

---

---

## **Links**

### **Software**

#### **Pest Patrol**

<http://www.pestpatrol.com/>

#### **Spyware Blaster**

<http://www.javacoolsoftware.com/spywareblaster.html>

#### **Spybot Search and Destroy**

<http://www.safer-networking.org/en/index.html>

#### **Adaware**

<http://www.lavasoft.de/software/adaware/>

#### **Webroot Spy Sweeper, Window Washer**

<http://www.webroot.com/>

## **Web Sites**

### **Spyware Info**

<http://www.spywareinfo.com/>

### **Spyware Warrior**

[http://www.spywarrior.com/rogue\\_anti-spyware.htm](http://www.spywarrior.com/rogue_anti-spyware.htm)

### **TeMerc Internet Security Site**

<http://groups.msn.com/TeMercInternetSecuritySite/malwarecountermeasures.msnw>

### **Scumware.com**

<http://www.scumware.com/>

### **Vic Laurie web site**

<http://vlaurie.com/index.html>

<http://www.vlaurie.com/computers2/Articles/spy.htm>

### **How many Spyware programs do you Need?**

<http://reviews.cnet.com/5208-6122-0.html?forumID=7&threadID=46126&messageID=546058>

### **What is Adware?**

<http://www.netlingo.com/lookup.cfm?term=adware>

### **What is Spyware?**

<http://www.netlingo.com/lookup.cfm?term=spyware>

<http://www.pestpatrol.com/pestinfo/>

### **What are Cookies?**

<http://www.netlingo.com/lookup.cfm?term=cookies>

### **What are Spyware Cookies?**

[http://www.pestpatrol.com/support/about/about\\_spyware\\_cookies.asp](http://www.pestpatrol.com/support/about/about_spyware_cookies.asp)

### **Rating Adware programs**

<http://www.adwarereport.com/mt/archives/000004.html>

### **Startup Programs**

[http://www.answersthatwork.com/Tasklist\\_pages/tasklist.htm](http://www.answersthatwork.com/Tasklist_pages/tasklist.htm)

[http://www.pacs-portal.co.uk/startup\\_index.htm](http://www.pacs-portal.co.uk/startup_index.htm)

**Task Manager** - <http://sysopt.earthweb.com/articles/TaskManager/>

**MSConfig** - <http://support.microsoft.com/default.aspx?scid=kb;en-us;310560>

<http://netsquirrel.com/msconfig/>