



Multi-State Information Sharing & Analysis Center (MS-ISAC)

Monthly Cyber Security Tips

NEWSLETTER

JUNE 2007

Volume 2, Issue 6

Recognizing and Avoiding Spyware

From the Desk of William F. Pelgrin, Chair

Spyware is a type of computer program that attaches itself to your operating system, generally without your permission or knowledge. It can be designed to track your Internet use, generate advertising pop-ups, take you to advertising sites, or sometimes even log information that you type into your computer. It can make your computer run extremely slow, bog down your network, or it could run quietly in the background and hardly be noticed at all. Spyware is a prevalent problem, and may even be infecting a majority of systems connected to the Internet. It is a problem that continues to grow for organizations and home users alike.

Below are some helpful hints from the MS-ISAC, OnGuard Online and the US-CERT on how you can protect your organization as well as your own system against the threat of spyware.

***Recognizing and Avoiding Spyware**

Because of its popularity, the internet has become an ideal target for advertising. As a result, spyware, or adware, has become increasingly prevalent. When troubleshooting problems with your computer, you may discover that the source of the problem is spyware software that has been installed on your machine without your knowledge.

***What is spyware?**

Despite its name, the term "spyware" doesn't refer to something used by undercover operatives, but rather by the advertising industry. In fact, spyware is also known as "adware." It refers to a category of software that, when installed on your computer, may send you pop-up ads, redirect your browser to certain web sites, or monitor the web sites that you visit. Some extreme, invasive versions of spyware may track exactly what keys you type.

Because of the extra processing, spyware may cause your computer to become slow or sluggish. There are also privacy implications:

- What information is being gathered?
- Who is receiving it?
- How is it being used?

*How do you know if there is spyware on your computer?

The following symptoms *may* indicate that spyware is installed on your computer:

- you are subject to endless pop-up windows
- you are redirected to web sites other than the one you typed into your browser
- new, unexpected toolbars appear in your web browser
- new, unexpected icons appear in the task tray at the bottom of your screen
- your browser's home page suddenly changed
- the search engine your browser opens when you click "search" has been changed
- certain keys fail to work in your browser (e.g., the tab key doesn't work when you are moving to the next field within a form)
- random Windows error messages begin to appear
- your computer suddenly seems very slow when opening programs or processing tasks (saving files, etc.)

*How can you prevent spyware from installing on your computer?

To avoid unintentionally installing it yourself, follow these good security practices:

- **Don't click on links within pop-up windows** - Because pop-up windows are often a product of spyware, clicking on the window may install spyware software on your computer. To close the pop-up window, click on the "X" icon in the titlebar instead of a "close" link within the window.
- **Choose "no" when asked unexpected questions** - Be wary of unexpected dialog boxes asking whether you want to run a particular program or perform another type of task. Always select "no" or "cancel," or close the dialog box by clicking the "X" icon in the titlebar.
- **Be wary of free downloadable software** - There are many sites that offer customized toolbars or other features that appeal to users. Don't download programs from sites you don't trust, and realize that you may be exposing your computer to spyware by downloading some of these programs.
- **Don't follow email links claiming to offer anti-spyware software** - Like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating.

As an additional good security practice, especially if you are concerned that you might have spyware on your machine and want to minimize the impact, consider taking the following action:

- **Adjust your browser preferences to limit pop-up windows and cookies** - Pop-up windows are often generated by some kind of scripting or active content. Adjusting the settings within your browser to reduce or prevent scripting or active content may reduce the number of pop-up windows that appear. Some browsers offer a specific option to block or limit pop-up windows. Certain types of cookies are sometimes considered spyware because they reveal what web pages you have visited. You can adjust your privacy settings to only allow cookies for the web site you are visiting (see [Browsing Safely: Understanding Active Content and Cookies](#) for more information).

*How do you remove spyware?

- **Run a full scan on your computer with your anti-virus software** - Some anti-virus software will find and remove spyware, but it may not find the spyware when it is

monitoring your computer in real time. Set your anti-virus software to prompt you to run a full scan periodically (see [Understanding Anti-Virus Software](#) for more information).

- **Run a legitimate product specifically designed to remove spyware** - Many vendors offer products that will scan your computer for spyware and remove any spyware software. Popular products include Lavasoft's Ad-Aware, Webroot's SpySweeper, PestPatrol, and Spybot Search and Destroy.

**Copyright Carnegie Mellon University, Produced by US-CERT*

Additionally, you should consider the following actions:

- **Use a firewall.** Ensure your system is protected by a network or personal firewall. For home systems, install a personal firewall to stop uninvited users from accessing your computer. A firewall blocks unauthorized access to your computer and, if properly configured, can alert you if spyware already on your computer is sending information out.
- **Ensure your operating system and its components are updated periodically.** Your operating system (like Windows or Linux) and browser (Internet Explorer, Firefox, Netscape, etc.) generally offers software "patches" to close holes in the system that spyware could exploit. Obtain these patches from your organization, or if your organization does not manage system updates, from the vendor's update site. Similarly, your firewall, anti-virus, and anti-spyware programs and signatures files should also be kept up-to-date. At home, consider using auto-update features to keep your operating systems and programs up to date.
- **Get Permission.** Remember at work to either request the installation through appropriate channels or obtain permission before installing programs on your organization's computers. Also, unlike anti-virus programs, most anti-spyware programs do not interfere with each other's operation, so using more than one anti-spyware program may be an option.
- **Remain vigilant** - No anti-spyware product removes all spyware programs, so you will still need to watch for signs of infection.

For more information:

<http://www.us-cert.gov/cas/tips/ST04-016.html>

<http://onguardonline.gov/spyware.html>

<http://www.microsoft.com/protect/computer/spyware/prevent.msp>

<http://computer.howstuffworks.com/spyware.htm>

Brought to you by:



<http://www.msisac.org>