



Reduce the likelihood of being infected with spyware:

- Carefully read the EULA before installing software, particularly 'free' downloaded software. Look closely for 'bundled' software that installs with the main program.
 - Don't click in/on advertising windows or boxes that pop-up when browsing. To close them, right-click its button on the task bar and left-click 'Close'
 - Don't click 'Yes' if unexpectedly prompted to run/install software or plugins.
 - Don't click on any link in, or reply to any spam (unsolicited email) message—particularly those that claim to scan your PC for viruses or spyware.
 - Adjust Internet Explorer security settings. Microsoft recommends security settings for the Internet zone of 'Medium' or higher. See [Working with Internet Explorer Security Settings](http://www.microsoft.com/windows/ie/using/howto/security/settings.msp) (<http://www.microsoft.com/windows/ie/using/howto/security/settings.msp>)
 - Use antivirus software, and update the virus definitions frequently (preferably daily)
 - Use an Internet Firewall
 - Keep your PC updated with the latest patches (Windows Update)
- Use an Anti-Spyware tool to regularly scan and clean your computer.

To detect and remove spyware:

Ad-Aware SE: www.lavasoftusa.com.

SpyBot S&D: www.safer-networking.org.

Be careful to type the URL (Web Address) exactly as listed—some unscrupulous companies use similar URLs to trick users into *installing* spyware instead of spyware removers!

Microsoft is also developing a free antispyware tool. As of this publication date, this software is 'beta' (test). If you are comfortable testing software, the URL is:

<http://www.microsoft.com/athome/security/spyware/default.msp>



NOTE: This is intended as a basic guide to illustrate some effective practices and some of the tools available to computer users. *Sinclair Community College does not endorse, or offer technical support for, any of the software or vendors listed in this document.*

Current as of April, 2005
Daniel V. O'Callaghan, Jr., CISSP
Chief Information Security Officer
<http://www.sinclair.edu/departments/infosec/index.cfm>
Sinclair Community College
444 West Third Street
Dayton, Ohio 45402



Spyware

What it is, Why it's a threat, and How to protect yourself.

Does your PC seem to be getting sluggish? Are you seeing an increase in pop-up ads, maybe even when you aren't using the Internet? Has your home page been changed, and does it resist letting you reset it? Do you have toolbars in your browser that you didn't install? Are they difficult to turn off or hide? Are you getting strange or unexpected results when searching the Internet?

**If any of this is happening to you,
your computer is very likely
infected with spyware!**

Spyware

What it is, Why it's a threat, and How to protect yourself.

What is spyware?

Spyware is a generic—and controversial—term for software that collects information about you and transmits this information to its “home”—often covertly. Some of this software (called *adware*) may be relatively harmless or even marginally beneficial as it simply tracks your Internet use habits to deliver targeted advertising; this allows some Web sites to remain free of charge. However, much of this software is more invasive and borders on illegal, capable of capturing personal, financial, and security (PINs & passwords) information, and transmitting this ‘home’ without the user’s knowledge or consent (this is truly *spyware*). Some spyware actually redirects all of the user’s Internet traffic through their ‘proxy’ server and captures every site visited and every action taken. The vast majority of these software applications fall in the middle-ground between adware and spyware, but a growing threat is illicit spyware applications that capture every keystroke, cause damage, abet identity theft, and/or hijack systems to turn them into spam ‘bots’ (robots).

Regardless of what the vendor calls it, the technology that powers adware and spyware is the same, and the end-user has little or no knowledge or control over specifically what information is being collected. From an information security perspective, this technology is all considered spyware.

Why is spyware a threat?

By design, spyware unobtrusively collects information from the users’ computer and transmits it to another computer. Even if the user has consciously accepted the EULA and understands that information is collected, the user has little or no ability to see or control exactly what information is being collected and sent, who is receiving it, and how it is being used. If data such as credit card numbers, bank account information, or passwords is harvested, even unintentionally, it is transmitted to the collecting computer.

Spyware technology can also do much more than simply harvest information. Because they are executable programs, spyware applications can be written to perform the same tasks as any other software programs. They may be written to create, modify, and access information stored on the hard drive, can snoop on other applications (such as email, word processing, financial management, messaging, and chat), can change what programs launch when your computer is turned on, hijack your Internet homepage (and resist changing it back!), and can even collect and transmit every keystroke. Even if the application does not initially do anything ‘harmful’ when installed, it may be susceptible to hacking and other attacks that can provide an intruder full control of the infected system. Because of the powerful abilities of spyware technology, it is rapidly becoming the tool of choice for criminals and other malicious individuals. Fraudsters such as ‘phishers’ are abandoning direct requests for personal information via email, and are instead using apparently benign messages to install spyware such as key-loggers, Trojan horses, and other malicious spyware applications.

How does a computer get infected with spyware?

Most spyware applications are ‘bundled’ with downloaded free software programs. The ‘free’ weather alert, screensaver, email virus scanner, game, or toolbar downloaded and installed also installs software that gathers information and reports to the sponsor. This is generally disclosed in the End User License Agreement (EULA)—the window with the ‘I Agree’ button that appears during installation—but is often buried in the fine print or is full of technical jargon the average user doesn’t understand. Specific details of what information is collected and how it is used are seldom found in the EULA.

Some of the illicit, most invasive, and dangerous spyware applications are installed via worms, viruses, and/or other exploits, but many are also increasingly installed when a user simply visits a Web site or clicks a pop-up advertisement (called ‘*drive-by*’ installation). Some unscrupulous individuals register Web addresses with names of popular products or legitimate sites; when a user lands on one of these pages, spyware is automatically installed. Pop-up messages used to install spyware include *Accelerate your Internet connection! Free email virus scanning software*, and even *Your computer may be infected with spyware-Scan Now!*

Users who click the pop-up or install the software advertised are then infected with spyware.

Current as of April, 2005

Daniel V. O’Callaghan, Jr., CISSP
Chief Information Security Officer

<http://www.sinclair.edu/departments/infosec/index.cfm>
Sinclair Community College
444 West Third Street
Dayton, Ohio 45402