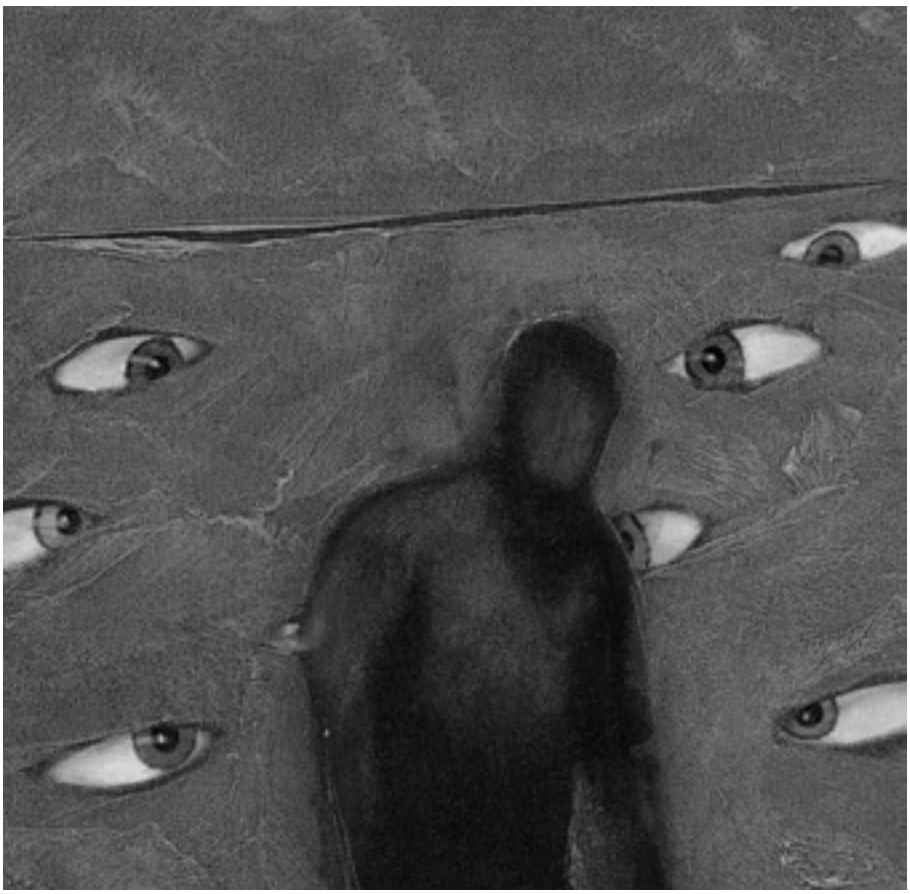
Monsters in the Closet: Spyware Awareness and Prevention

Despite the stealthy nature of the threat, you can take measures to remove spyware from your system and prevent reinfection

By **Christofer Sean Cordes**



You are an instructional technologist, in charge of all your organization's Web pages. You are making some last-minute changes before your colleagues, including your boss, preview your new site design.

You start to type a URL to the home page when you notice your code is not appearing in the editor, and advertisements are popping up like crazy in the background. With some effort you close all the ads, make your changes, and save the file. The presentation begins. You click the home button on the browser, but instead of your new home page design, you—and your audience—are transported to … a porn site.

Sound farfetched? Not with the policies and capabilities of today's Web environment. Some Internet technologies and delivery methods—known collectively as spyware, many of them legal and free—can wreak havoc on the best-laid technology programs and plans. But what is spyware, what does it do, and how can you prevent it from affecting your educational organization's operations?

Spyware is the general term that describes a collection of technologies that help external parties in "gathering information about a person or organization without their knowledge."[1] In addition to the minor annoyances spyware generates, such as redirected pages, redirected searches, and pop-up ads, a spyware infection can have more malicious effects, including the gathering of personal information from unwitting users—e-mail addresses, credit card numbers, and even passwords. Further, some spyware has the ability to read the files on your hard drive, track the strokes you make on your keyboard, and even track the use of other applications, like chat rooms. Finally, spyware infection can lead to slow Internet connections and system instability and crashes.

Computers typically become infected with spyware from tainted freeware and shareware programs, including peer-to-peer applications like those used for sharing music and movies. Like other types of malware (malicious software), spyware is installed along with the intended application and without the user's knowledge.[2] A broad range of spyware categories and products are currently at large.[3] Common types of spyware you might run into on your organization's network or Web space include adware, browser hijackers, browser plug-ins, keyloggers, and phishers.

■ *Adware*
Adware creates the annoying pop-ups that infest your desktop and browser window. Typically legal programs that run in the background, they hold down the cost of Web site operations and maintenance. At best, adware is a cause of distraction and workflow slowdown; at worst, adware includes code that tracks personal information and passes it on to third parties without the user's authorization or knowledge.

■ *Browser Hijackers*
A browser hijacker changes settings in your browser. If you find that your search page or home page setting has changed, you might have a hijacked browser. Browser hijackings are a nuisance because they often replace your free search service with a fee-based or otherwise unfamiliar search page. In addition, they can send you to offensive pages, such as porn sites.

■ *Browser Plug-Ins*
Browser plug-ins typically add toolbars to your browser. A common browser plug-in is the "Search Assistant" toolbar. Some browser plug-ins transmit personal information without the user's knowledge.

■ *Keyloggers*
Keylogger programs track user activity. Many keyloggers are sold commercially for a number of legitimate reasons, including ensuring user safety or monitoring employee Web use. Used without the user's knowledge, keyloggers can compromise individual and organizational privacy.

■ *Phishers*
Phishing programs use fake Web sites and e-mails (spam) to trick users into giving out private information like credit card numbers, account user names and passwords, and Social Security numbers. Phishers lure users to harm by mimicking the names and appearance of trusted Web sites and organizations. Once users feel safe, they often unwittingly give up personal information to the "phishers."

Fortunately, in response to spyware threats, a growing number of programs, services, and procedures are available. Many of these are free.

An Ounce of Prevention

Fortunately, in response to spyware threats, a growing number of programs, services, and procedures are available. Many of these are free, and they can help keep your Web space running smoothly. Some sites like Spykiller.com allow you to scan your machine for spyware free but charge a fee to unlock the removal feature of their product.[4] These services help in identifying problems, but other solutions are available at a lower cost, though they are not always as comprehensive.

Maybe most useful for the technical novice or systems librarian on the go are the multitude of freeware and shareware programs that remove spyware. Lavasoft's Adaware is a free utility that has a sound reputation as a leader in the battle against unwanted intrusions.[5] Others, like Spybot Search and Destroy, are more effective for a broader range of spyware, like keyloggers, tracking cookies, and many registry-changing data objects.[6] Also, although they do not remove spyware, some browser add-ons can help eliminate negative spyware experiences. One such add-on is the Google Toolbar with Popup Blocker.[7] Another is SpoofStick, a utility that opens in the browser to alert users about fake Web sites used by phishers.[8]

Still, some spyware programs require more specialized methods of prevention and removal, like manual adjustments of computer settings or the program directory (accessed through the Add and Remove programs in Windows) to clear spyware from the local machine. To address this need, sites like 2-Spyware.com provide free step-by-step instructions for removing spyware, particularly those spyware programs that require manual adjustments to the computer registry.[9]

There are many reasons to fear a spyware infestation in your library and university Web systems. But with the proper tools, prevention processes, and a bit of common sense, you can make the fight a lot more effective. The following points can help practitioners keep spyware issues in perspective.

The Good, the Bad, the Ugly

Not all spyware is bad. In fact, most is fairly benign, and some can even be quite helpful. Commercial Web sites like Amazon.com frequently gather information through cookies that remember user preference so that they can provide a more effective experience when an online shopper returns to the site. Also, some commercial keylogging programs can help ensure that Internet services are used appropriately in libraries, including tracking patron Web site travels and even monitoring staff in some cases to deter time-wasting personal Web surfing. Still, without awareness and monitoring, beneficial applications can quickly turn to serious privacy threats, especially in public facilities. For example, the FBI, once an in-house developer of surveillance spyware, now uses commercial spyware to monitor Internet activity. This includes patron activity on computers in libraries. Further, these same methods may be used to monitor library staff machines, without physical access and without the staff member's knowledge.[10]

Time Does Not Heal All Wounds

Time can be both a blessing and a curse when dealing with spyware. On one hand, a single spybot will rarely disrupt work enough initially to cause an immediate slowdown in computer performance. Nor will it cause an immediate shutdown of your machine in most

cases, like some computer viruses do. This delay of onset can give the systems librarian time to research and remove spyware from the system.

On the other hand, without ongoing vigilance, spyware can infest machines across the library system, slowing production to a crawl, generating pop-ups faster than a mole in an arcade game, and sending users to places they never wished to visit. By the time you notice anything odd, it might be too late for an easy fix. Luckily, the symptoms of infection are—for the moment—documented. Some of the more common oddities to notice when diagnosing a spyware infestation include:

- *Home and search page eviction*. You type in or hit your home page buttons, only to find yourself on an unknown home page. Likewise, "page not found" errors redirect you to the spyware spammers' search page.
- *Snail syndrome slowdown*. Programs creep along, windows open and close in bits and pieces, things just don't run smoothly. You know your machine best; if it is not its normal spunky self, it might be infected.
- *New—and unexpected—favorites*. Some spyware will add new entries into your browser's favorites folder. This creates clutter and potentially inappropriate folder entries.
- *Stroke-by-stroke surveillance*. Keylogger spyware can capture user names, passwords, and PIN information from your machine or online forms, then use this information later online. If you notice changes to important numbers, you might be the victim of a keylogger attack. Other malware programs can write their commands into your registry.
- *Fishy pop-ups*. Spyware software can generate pop-up ads that appear to be from familiar businesses to lure you to their dubious sites. These are not to be confused with phishing, a technique used to lead users to sites with URLs similar to popular sites.
- *E-mail errata*. Trojan spamware can return e-mail messages as undeliverable, deny delivery of outgoing e-mail, send its own e-mail from your machine, or steal your e-mail address from your machine. If you notice e-mail messages are not coming or going as they should, you may want to dig a bit deeper.

This list highlights some of the most common symptoms, but is far from complete. As technology marches on, spyware developers are creating more pests, and users are becoming aware of still more symptoms. For example, the *Intranet Journal Online* warns against insidious "Noises, Bells, and Whistles," where Trojan-horse programs can put a poltergeist into your machine. Hard drives spin for no data-driven purpose, and mysterious icons appear in the system tray.[11] Further, GetNetWise cautions computer users to watch for misuse of 900 numbers reviewing telephone charges. Notice any questionable toll calls lately? A new evil on the spyware front, 900 dialers will disconnect your Internet session and redial toll numbers through the machine without your knowledge.[12]

Rarely a Single Solution

There really is no cure-all solution for spyware. Some programs like Lavasoft's Adaware are great for detecting and removing certain types of spybots. Others, like Spybot Search and Destroy, offer a broader range of prevention. And browser extensions like the Google Toolbar and SpoofStick are great for targeting and eliminating pop-ups and fake Web site redirections. Currently, I run Adaware and Spybot Search and Destroy at least once a week on all my machines. In addition, I routinely check my registry and programs for unfamiliar entries. Rarely a week goes by that I find nothing amiss.

The best practice, though, is a routine maintenance schedule using a variety of spyware removal tools and methods, similar to the virus prevention measures taken in most library systems now. If you are an educational or instructional technologist responsible for all your school or departmental Web systems, you may have the authority to conduct this maintenance on your own. If you are part of a larger organization, check first to see what policies your library, school, or university have for detecting and preventing spyware. If there are none currently in place in your organization (or home), I suggest a few measures:

- Instruct users and staff about the warning signs and seriousness of spyware infection.
- Use a firewall system-wide and on individual machines.
- Install antivirus software and keep it current with the latest subscriptions and versions.
- Instruct patrons not to input personal and confidential information on library computers or to log out after doing so.
- Install and run anti-spyware and anti-adware applications before opening any programs.
- Begin an ongoing, comprehensive detection program using proven spyware detection programs such as Spybot Search and Destroy, Adaware, AntiKeylogger, and Trojan Monitor.

The Future Is Yesterday

Spyware is a growing problem for a number of reasons, including a lack of regulation, more-complex Internet security issues, and a lack of user awareness. Recently the issue caught the attention of U.S. legislators. In response to the problem a bill has been introduced to Congress to protect users. Named the Software Principles Yielding Better Levels of Consumer Knowledge Act, or SPYBLOCK, the bill is designed to inform users about the software they load and give them more control over the activity occurring on the computer, including user-friendly ways to remove software after installation.[13] Yet despite its promise, many are concerned that the bill's strength lies with the power it grants to the Federal Trade Commission regarding spyware use, and not directly with the user.[14] Still, this is not to say that many organizations aren't already taking spyware prevention measures.

Dell recently partnered with the Internet Education Foundation to develop the Consumer Spyware Initiative, a campaign to raise public awareness about spyware in the Internet community, with the goal of reaching 63 million Internet users.[15] Regarding

spyware issues in higher education, a quick MSN Web search for "spyware and university" returns a number of results reflecting measures being taken across the country at institutions such as Duke University, Marquette University, Howard University, and the University of Wisconsin, among others.[16] So, for now, the best practice for prevention may be advancing free, open source solutions and an extra degree of vigilance and maintenance for our systems at home. *e*

Endnotes

1. From the SearchCIO.com site, searching for the term spyware, <http://searchcio.techtarget.com/sDefinition/0,,sid19_gci214518,00.html> (accessed February 7, 2005).
2. Find the Webopedia dictionary definition of spyware at <http://www.webopedia.com/TERM/s/spyware.html> (accessed February 7, 2005).
3. SpywareGuide.com, consult the Spyware Guide Database for spyware, adware, and malware, <http://www.spywareguide.com/index.php> (accessed February 7, 2005).
4. Swansoft Technologies, Inc., Spykiller.com, <http://www.spykiller.com/>.
5. See the Lava Software, Inc., press releases, <http://www.lavasoftware.com/pressreleases.html> (accessed February 7, 2005).
6. For an explanation of Spybot, see P. M. Kolla, "Spybot—Search and Destroy," <http://www.safer-networking.org/en/spybotsd/index.html> (accessed February 7, 2005).
7. Google.com, Google Toolbar, <http://www.toolbar.google.com/>.
8. CoreStreet Ltd., SpoofStick home page, <http://www.corestreet.com/spoofstick/>.
9. See 2-Spyware.com for instructions on how to remove spyware and adware, <http://2-spyware.com/>.
10. T. Bridis, "FBId Stops Using Carnivore Wiretap Software," Information Week, story dated January 19, 2005, <http://www.informationweek.com/story/showArticle.jhtml?articleID=57702375> (accessed February 10, 2005).
11. "Symptoms of Spyware and Other Pests," *Intranet Journal Online*, <http://www.intranetjournal.com/spyware/symptomspr.html> (accessed February 7, 2005).
12. GetNetWise, "Symptoms of Spyware," <http://spotlight.getnetwise.org/spyware/tips/symptoms> (accessed February 7, 2005).
13. On the Senate.gov site for Senator Conrad Burns, Montana, see the press release dated February 26, 2004, <http://burns.senate.gov/index.cfm?FuseAction=PressReleases.View&PressRelease_id=1077> (accessed February 7, 2005).
14. E. Hill, *CNN.com*, "New Bill Aims to Shine Light on Spyware," story dated March 3, 2004, <http://www.cnn.com/2004/TECH/03/03/hln.wired.spyware/> (accessed February 7, 2005).
15. T. Dingboom, press release dated October 15, 2004, "Internet Education Foundation, Dell Launch Consumer Spyware Initiative," Dittus Communications, Washington, D.C., <http://www.getnetwise.org/press/2004pressrelease> (accessed February 7, 2005).
16. MSN Web search for the term "spyware and university" August 2004, <http://search.msn.com/results.aspx?FORM=MSNH&q=spyware%20and%20university> (accessed again February 7, 2005).

Christofer Sean Cordes (scordes@gwgate.ib.iastate.edu) is Assistant Professor and Instructional Technology Librarian at Iowa State University in Ames, Iowa.