Chapter 5

Getting Rid of Unwanted Guests, Part 2: Spyware, Adware, and Trojan Horses

The preceding chapter discussed the rise of malware and examined two particular species of malware: viruses and worms. This chapter examines three other distinct kinds of security risks: spyware, adware, and Trojan horses. We'll spend some time defining each of these risks, look at the legal and technological challenges of dealing with spyware and adware, and discuss how to protect yourself from these threats.

5.1 What Are Spyware, Adware, and Trojan Horses?

In a narrow sense, spyware is a term for some tracking technologies (specifically, executable applications) deployed on your computer without adequate notice, consent, or control. Spyware can monitor your activities online and/or perform functions without your knowledge or consent. Depending on the program, spyware can track and report on every Web site you visit, generate pop-up advertising, change your home page and browser settings, or record every key you press. In its broader sense, spyware is also commonly used as the overall name for most types of potentially unwanted technologies detected by popular anti-spyware programs. These technologies are implemented in ways that impair your control over

the following: collection, use, and distribution of your personal information; material changes that affect your desktop experience, privacy, or system security; and use of your system resources. These are items that users of anti-spyware software will want to be informed about and that they may want to easily remove or disable.

Adware is a subset of the broader spyware category, which is designed to deliver targeted advertising to your Web browser, especially through the use of pop-up ads. Adware is often bundled with other software programs, such as peer-to-peer file-sharing software, games, or other utilities that can be downloaded for free from the Web. Adware knows what kinds of ads to deliver to you because it tracks the places you surf. For instance, if you surf to a car rental site, an adware program might generate a pop-up ad that a competing car rental company has paid the adware company to deliver to you. Besides tracking your behavior and annoying you with ads, adware may also open a connection on the Internet to report your surfing habits back to a central server. This information, which may include your age, your sex, your shopping habits, and even your location, is used to conduct "market research" to attract new clients.

Trojan horses are programs that claim to be something they are not. For instance, a Trojan horse may advertise itself as an amusing animation clip, a screen saver, or a free software program that promises to do something cool or helpful. But Trojan horses also include unadvertised functions (if, in fact, the advertised function works at all). The most common goal of a Trojan horse is to install a back door on your computer or steal passwords. A back door lets attackers control your machine remotely. Some classes of spyware can be considered Trojan horses because they arrive under false pretenses. For instance, you may have downloaded a neat little screen saver with pretty butterflies on it that also happens to monitor your Web-surfing habits or log your keystrokes. Trojan horses often rely on viruses, worms, and social engineering to get unsuspecting users to download them.

The term Trojan horse has become shorthand for any program that resides on your computer and provides remote access to an unauthorized person or performs unwanted functions. Most anti-virus (AV) software and some anti-spyware software can detect Trojan horses.

Spyware, adware, and Trojan horses can't replicate themselves. Thus, these categories of applications need other ways to spread. For instance, Trojan horses may be delivered as part of the payload of a worm or virus, included as an e-mail attachment, or bundled with other software. Spyware and adware use similar techniques to spread, but they are most frequently downloaded as part of a "free" file-sharing program or software utility or via drive-by downloads (in which you visit a Web site that installs the program without your permission).

Defining Spyware and Adware

While security risks such as spyware and adware can be seen as an extension of the virus problem, there are significant differences in how these programs are judged as desirable or undesirable and whether you want them on your machine. Viruses, worms, and Trojan horses are always undesirable and should be automatically removed from a computer. Many types of programs classified as adware and spyware are also high-risk and can have a significant negative impact on computer performance or invade your privacy by transmitting personal information to a third party.

However, other adware programs are low-risk. They can deliver useful functionality such as games or utilities and have a relatively small impact on privacy and computer performance. Just as broadcast television programs are free because television companies earn revenue from advertising, many software programs are free to download because they too rely on advertising to generate income. Such software programs are called ad-supported programs. They include adware to deliver targeted ads. Some ad-supported software programs seek the user's consent before installing adware; others do not. Still others operate in a gray area in which user consent is part of the "fine print" of a software license agreement. We'll examine these distinctions and what they mean to you more closely in subsequent sections.

The broad range of spyware and adware or potentially unwanted programs can be divided into two general categories: high-risk or malicious programs and low-risk programs. Security researchers assign spyware and adware programs to one of these categories depending on how the programs are installed, what data they try to export from your computer, what impact they have on your computer's performance, and what you are led to understand about their operation and intent. When security researchers investigate a program's behaviors to determine risk, they look at a number of key areas, including installation characteristics, stealth properties, privacy impact, integrity impact, performance impact, and ease of removal:

- Does the program impact system stability or slow down the network connection?
- Does the program launch pop-up advertisements? If so, how frequently?
- Does the program serve as a means of downloading and installing other security risks (such as additional spyware and/or adware)?

- Does the program replace the browser home page or alter search options or behavior?
- Does the program cause the release of confidential, sensitive information such as bank account numbers and passwords?
- Does the program cause the release of less-sensitive data such as tracking of Web-surfing habits?
- Does the program have a privacy policy, and does its behavior match the stated policy?
- Does the program try to hide itself or avoid being uninstalled by the user, including an unsolicited reinstallation and techniques to restart user-terminated processes?
- Does the program lack an uninstall feature or fail to register in the Microsoft Windows Add or Remove Programs area?
- Does the program install itself silently, with little or no indication to the user?
- Does the program lack a user interface?
- Does the program conceal its processes or hide them from the user using an obscure name?
- Is the user notified of the program's presence only through an End User License Agreement (EULA)? Does the EULA appear to relate to a different program?

To qualify as high-risk or malicious spyware and adware, programs must have significant impact on system stability and/or performance or release confidential, sensitive information and/or exhibit stealth behaviors such as a silent installation, no user interface, and concealment of application processes. Examples of high-risk programs can include keystroke loggers, browser hijackers, and dialers. (Table 5.1 describes these and other kinds of programs.) Malicious spyware is illegal and therefore is employed by criminals who want to steal from you. Malicious spyware gets installed on your computer through software vulnerabilities, worms and viruses, social engineering, and drive-by downloads.

Low-risk programs include many popular commercial adware or ad-assisted programs. However, some adware generates multiple pop-up ads and performs other unwanted functions, like changing your home page, directing you to unfamiliar search engines, or installing toolbars in your Web browser that you didn't

Table 5.1

Spyware Definitions

Term	Definition
Spyware	Spyware is a general class of software programs that monitor computer activity and relay that information to other computers or locations on the Internet. Among the information that may be actively or passively gathered and transmitted by spyware are passwords, log-in details, account numbers, personal information, individual files, and personal documents. Spyware may also gather and distribute information related to the user's computer, applications running on the computer, Internet browser usage, and other computing habits. Spyware is usually loaded onto a user's computer without the user's knowledge and is created by underground attackers or criminals.
Adware	Adware is a type of advertising display technology—specifically, executable applications whose primary purpose is to deliver advertising content. Many adware applications also perform tracking functions and therefore may also be categorized as tracking technologies. Consumers may want to remove adware if they object to such tracking, do not want to see the advertising generated by the program, or are frustrated by its effects on system performance. Some users might want to keep particular adware programs if their presence is a condition for the use of other free software. Adware is created by commercial software companies rather than criminals and is often bundled with popular free software, such as file-sharing programs. Some adware describes its functions in a license agreement and provides uninstall options; other adware may install itself without a user's permission and thwart attempts at removal.
Keystroke logger (also known as a keylogger)	Keyloggers are tracking technologies that surreptitiously record keyboard activity. Keyloggers typically either store the recorded keystrokes for later retrieval or transmit them to the remote process or person employing the keylogger via e-mail. Keystroke loggers are used to steal passwords and other identity information.
Browser hijacker	Browser hijackers reset your home page and redirect your browser to unwanted or unknown search engines or other Web sites. Some browser hijackers can prevent you from restoring your home page. Browser hijackers work by deleting the entry for the home page you've selected and inserting their own in a special file that your computer consults (the hosts file). They also might intercept search queries typed into a legitimate search engine and display their own results.

Term	Definition
Browser Helper Object (BHO)	BHOs are companion applications for Microsoft Internet Explorer (IE) that run automatically whenever IE is launched. They are a form of state management tool. Many tracking technologies or advertising display technologies are implemented as BHOs. BHOs can search the Web pages a user visits and replace banner ads generated by the Web server with targeted ads. BHOs can also monitor and report on a user's surfing behavior and may reset a user's home page. Note that not all BHOs are malicious; many legitimate Web browser toolbars are BHOs.
Trojan horse	Trojan horse software masquerades as an innocuous or useful program to trick a user into installing it. Once installed, the Trojan horse engages in unwanted or unadvertised functions.
Remote Access/ Administration Tool (RAT)	RATs are executable applications designed to allow remote access to or control of a system. They are a type of remote-control technology. Many legitimate uses of RATs do not pose security threats, but they can be used maliciously, especially when used by someone other than the computer's legitimate owner or administrator.
Dialer	Dialers are programs that use a computer's modem to make calls or access services. Users may want to remove dialers that can result in unexpected phone numbers being dialed or unexpected telephone charges. Dialer is a colloquial term for dialing technologies.

seek out and don't want. Adware may also read cookies installed on your computer to find out information about you and your Web habits.

Of course, regardless of whether a program is high- or low-risk, you, the user, should have absolute control over the programs on your computer, including the ability to find and remove any programs you don't want. As you'll see in the following section, some spyware and adware attempts to usurp that control.

5.2 Technical and Legal Challenges of Detecting and Removing Spyware and Adware

Chapter 4, "Getting Rid of Unwanted Guests, Part 1: Viruses and Worms," talked about several reasons for the rise of malware (ease of communication, a homogenous computing environment, reactive security software). Those factors certainly apply to the rise of spyware, but the undeniable *raison d'être* of spyware and adware is money. Whether facilitating identity theft, recruiting your computer

into a rentable bot network, or generating advertising revenue for shady software companies, this type of application is increasingly influenced by dollar signs. The potential profits that can be generated make the spyware/adware problem inherently more difficult to solve. Spyware brokers can hire programmers to continually tweak the code to better avoid detection and removal by security software or encourage the development of open-source or professional library programs.

Just how profitable a business is it? Consider this: An adware company called Claria earned approximately $90 million in 2003. (Claria's adware products are known as GAIN or Gator, and they often come bundled with third-party software such as Kazaa, the peer-to-peer software.) With profits like this, adware companies have strong motivation to continue what they are doing. Other adware companies include WhenU., 180Solutions, Avenue Media, and Direct Revenue.

Numerous indicators demonstrate the pervasiveness of spyware and adware. The Internet service provider (ISP) Earthlink conducted a study with WebRoot, which makes anti-spyware software. They scanned more than 3.2 million PCs and found an average of 26 spyware programs per PC. Dell Computer says spyware problems are the number one cause of tech support calls. Symantec conducted a study to see which categories of Web sites left behind the most unwanted software. Researchers took a brand-new Windows PC out of the box, connected it to the Internet without any standard protection software, and browsed. Testers spent one hour each interacting with different categories of Web sites. Surprisingly, children's Web sites dumped the most unwanted software on a PC—359 pieces of adware in just an hour's surfing. By comparison, the second-highest total was 64 pieces of adware installed from travel sites. Gaming sites dumped the most spyware—four pieces. Table 5.2 lists the full results.

Table 5.2

Symantec's "Unwanted Software" Study

Site Category	Adware	Spyware	Hijackers	Cookies
Gaming	23	4	2	68
Kids	359	0	3	31
News	3	1	0	26
Reseller	2	1	1	22
Shopping	0	0	0	10
Sports	17	2	0	72
Travel	64	2	1	35

Creators of high-risk adware and spyware tend to make their software difficult to find and get rid of. For instance, a spyware program may put thousands of files on a PC and make thousands of changes to the Registry. The Registry is a database of configuration settings that tells the computer about the applications and user profiles on your machine. Your computer refers to the Registry at startup and each time you open programs. Spyware and adware often insert themselves into the Registry to become one of the programs that the computer runs automatically.

Spyware and adware may put two copies of themselves on your PC so that if you delete one, the backup copy will still run. Or they may plant "tricklers" on your computer. Tricklers are tiny pieces of software that download unwanted programs a little bit at a time each time the computer is connected to the Internet, until the entire program is installed.

Legitimate software is relatively easy to uninstall using the Add or Remove Programs function in Windows XP, shown in Figure 5.1. It basically lists all the programs on your computer and gives you the option to uninstall each one individually. One of the indicators of a high-risk adware or spyware program is that it doesn't appear in the list of programs. To see the list of programs on your PC, click the Start button and then choose Add/Remove. If Add/Remove is not on your Start menu, choose Control Panel and then Add or Remove Programs. A legitimate adware program would appear in this area and allow you to remove it.

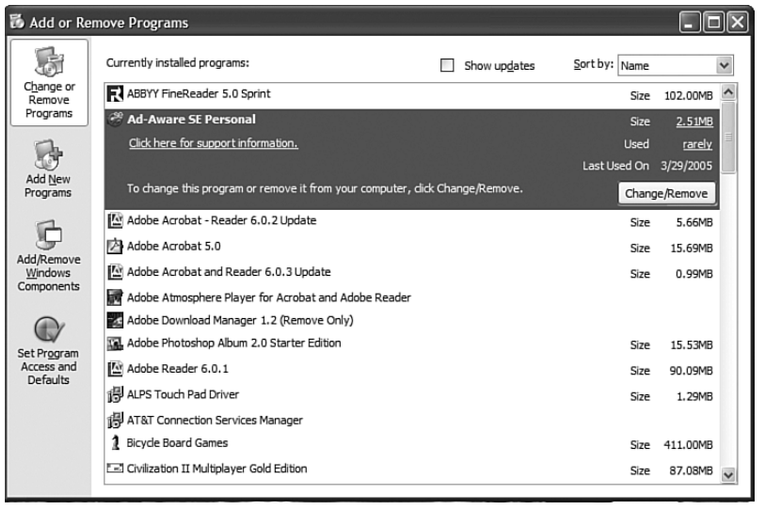

Figure 5.1 Add or Remove Programs.

Some spyware even goes so far as installing itself without your permission (for instance, even if you click "No, I don't want this program," it still installs itself) or without your knowledge (a drive-by download). All of these characteristics make spyware and adware difficult to find and remove.

Some adware companies claim they are trying to become better Internet citizens. For instance, Claria and WhenU. say they have sworn off dirty tricks like drive-by downloads to install their software on consumers' PCs. (But some researchers argue they still make it difficult for users to find and uninstall their programs.)

Other adware vendors don't even bother with appearances of legitimacy and continue to play dirty, even with each other. For instance, in 2004, Avenue Media accused DirectRevenue of creating software to find and remove Avenue Media's adware and install its own on consumer PCs.

Besides the technical challenges of preventing and removing spyware and adware, there are also legal issues to deal with. While some categories of spyware are overtly against the law (such as keystroke loggers), adware enjoys a quasi-legal status. For instance, any adware that notifies users of its functions in a EULA is, for the most part, legal. That's because you, the user, are supposed to read and agree to the conditions contained in the EULA. Before the download commences, you must click a button that says something like "I agree to the terms and conditions set forth in this license." Clicking such a button is akin to signing a physical contract; once you click yes, you agree to whatever the EULA says. However, almost no one bothers to read EULAs, and the adware companies know it. (See the sidebar at the end of this chapter, "Reading the Fine Print," for more information.)

Its advisable to seek out and read the EULA for any sites you visit or programs you download. If a program has no EULA or tries to hide its intent behind confusing language, take this as a warning sign, and strongly consider not downloading the program.

However, one of the issues under debate regarding adware EULAs is figuring out what constitutes sufficient notice and consent. If an adware program actually describes its functions in a EULA, does that count as sufficient notice? What if that description is buried inside a long agreement and is vaguely or confusingly worded?

A number of federal legislative solutions have been proposed recently to address spyware and adware, including the issue of sufficient notice and consent. As of June 1, 2005, two bills had been introduced in the House and two in the Senate. In the House of Representatives, legislation known as the SPY ACT (Securely Protect Yourself Against Computer Trespassers, H.R. 29), is sponsored by Congresswoman Mary Bono. The SPY ACT would generally make unacceptable behavior, such as installing software without your permission, illegal. The bill also stipulates that adware vendors must clearly state the software's functions, the types of information being collected, and the purposes for collecting the information. The bill also says adware must give consumers the ability to decline installation or remove the software at any time without "undue effort." Another House bill, the I-SPY Prevention Act of 2005 (H.R. 744), was introduced by Congressman Bob Goodlatte on February 10, 2005. It focuses largely on taking enforcement action and stiffening penalties against the bad guys. This bill adds a new Section 1030A to the Criminal Code titled "Illicit indirect use of protected computers" and creates three criminal prohibitions.

In the Senate, the SPY BLOCK Act (S. 687) was introduced by Senator Conrad Burns with Senators Ron Wyden and Barbara Boxer on March 20, 2005. The Act would prohibit installing software on somebody else's computer without notice and consent and requires reasonable uninstall procedures for all downloadable software. The Enhanced Consumer Protection Against Spyware Act of 2005, introduced by Senator Allen with Senators Smith and Ensign on May 11, 2005, would allow for the seizing of profits from companies and individuals secretly installing spyware on computers. It would seek significantly higher civil and criminal penalties for those trafficking in spyware. It also would beef up the Federal Trade Commission's authority to prosecute spyware intrusions.

All four of the bills recognize that many of the technologies used for malicious and deceptive practices can also be used for beneficial and legitimate purposes. According to the legislation, being adware or spyware doesn't necessarily make the technology bad or illegal. The bills only seek to regulate the misuse of adware and spyware.

As of June 1, 2005, H.R. 29 and H.R. 744 had both been passed in the House. What remains is for the Senate to vote on its own two bills, and then for the House and Senate to agree on a combined bill that would pass both houses. Finally, the president would have to sign the bill into law.

You can read all four bills by going to Thomas, a search page run by the Library of Congress for finding legislation online. Go to http://thomas.loc.gov and type the bill's name or number into the search field for the 109th Congress.

In addition to the federal legislative activity this year, more than 40 spyware bills have been introduced in state legislatures.

The Federal Trade Commission has also taken notice of the spyware problem. In March 2005, the commission released a report titled "Monitoring Software on Your PC: Spyware, Adware, and Other Software." The report outlines the problems associated with defining spyware, the risks spyware presents to consumers, and how government and industry leaders can respond to the spyware problem. To find a copy of the report, see the "Helpful Resources" section near the end of this chapter.

Legal issues have also complicated the efforts of anti-spyware vendors to deal with adware. In 2003, Claria sued PC PitStop, an anti-spyware organization, for defamation. PC PitStop was calling Claria's products spyware, and the company didn't appreciate it. In 2005, the makers of the popular WeatherBug software complained when Microsoft's anti-spyware product listed an ad-serving component inside WeatherBug as a privacy risk. Microsoft reviewed the complaint and removed the signature that detected the ad server.

Some anti-spyware products have found themselves at cross-purposes with other business units inside the same company. The online portal Yahoo! offers a free anti-spyware program in its Yahoo! toolbar. But when the product was first launched, it required users to specifically request a scan for adware in addition to spyware. That's because Yahoo!'s Overture division, which provides paid search listings, is a business partner of Claria Corporation. According to a June 2004 story in *eWeek,*[1] Overture provided paid listings to SearchScout, a Claria service that displays "pop-under" advertising. (These ads show up under the page; you see them after you close the browser.) SearchScout was responsible for 31 percent of Claria's revenue in 2003. Yahoo! has since changed its anti-spyware toolbar to search for adware in addition to spyware.

One way for anti-spyware companies to avoid trouble is by adopting more diplomatic language. For instance, McAfee's anti-spyware software uses the term

1. "Yahoo Plays Favorites with Some Adware," by Matt Hicks, published on June 1, 2004 in eWeek (www.eweek.com).

"Potentially Unwanted Programs" rather than "adware" or "spyware." Microsoft's anti-spyware software also skirts the issue by referring to everything as "Potentially Unwanted Software." (If you turn that into an acronym, it spells PUS. I don't know if the folks at Microsoft chose it on purpose, but it generally sums up the feelings of people who have to deal with this kind of thing. It's also shorter than my own term, which also can be turned into an acronym: Bad, Annoying Software That All of us Require be Deleted Speedily.)

Do You Want a Cookie?

Cookies present another difficulty with classifying and dealing with intrusive or unwanted programs. Cookies are small text files that a Web server places on your computer when you visit a Web site. Cookies contain information about you such as your user preferences or log-in information. Each time you return to a Web site, the appropriate cookie is transmitted from your computer to the Web site to help customize your visit. For instance, if you're a regular customer of an e-commerce site, that site might store information about you in a cookie on your PC, such as your shopping history, purchase preferences, and so on. Cookies facilitate the e-commerce experience and generally are benign.

However, another category of cookie, called a tracking cookie, records information about other Web sites you visit and shares that information with other sites. Advertising networks collect this information to conduct market research and help them serve targeted ads on your computer. Good anti-spyware software should detect tracking cookies and give you the option of deleting them.

You can see the cookies on your computer by going to My Computer. Click the Local Disk (C:) folder, then Documents and Settings, then your username, and then the Cookies folder. However, looking at cookies won't tell you much about whether it's a standard cookie or a tracking cookie. Most cookies consist of lots of numbers that have meaning to a Web server, but not a human. However, by looking at the Cookies list you can see which Web sites are setting cookies on your hard drive. You can delete them by highlighting the specific file and clicking the Delete this file command on the left side of the window, as shown in Figure 5.2.

Figure 5.2 Deleting cookies.

You also can control how and whether Web sites can set cookies on your computer by adjusting your privacy settings in your Web browser. If you're using Internet Explorer, open the browser and select Tools, Internet Options, Privacy. A slider bar adjusts the privacy setting and tells the Web browser what kinds of cookies it accepts, as shown in Figure 5.3. Options range from accepting all cookies to blocking all cookies, with various gradations in between. Microsoft's default setting is Medium High, which means your browser blocks any cookies that attempt to use personally identifiable information without your explicit consent.

Remember, not all cookies are invasive. For instance, if you delete cookies from e-commerce sites you use regularly, you may find that the customization you enjoyed has been wiped out. Also, setting your cookie protection too high might lock you out of sites. For instance, my Yahoo! Web mail account wouldn't work with the Block All Cookies or High security settings in Internet Explorer. Cookie setting is discussed in more depth in Chapter 7, "Securing Windows."

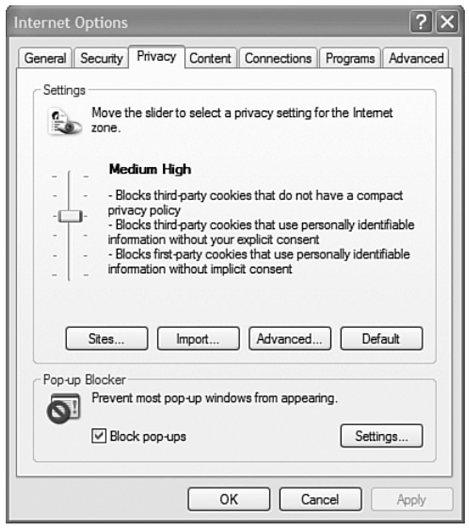

Figure 5.3 Setting cookie options in IE.

Another example of such tracking objects are Local Shared Objects (LSOs), which are best thought of as Macromedia Flash program cookies. A Web site can use an LSO to store information on your computer such as a game's high score or information you have filled in (such as your name and age). Unlike with a cookie, however, you cannot disable LSOs through your normal browser settings.

5.3 How Spyware/Adware and Trojan Horses Infect Your Computer

Spyware, adware, and Trojan horses can get onto your machine in a number of ways, including from a Web browser, via e-mail, or in a bundle with other software you download. By knowing how this software gets on your machine, you'll have a better idea of how to keep it out.

From a Web Browser

One of the reasons that Web browsing is a popular spyware/adware vehicle is ActiveX. ActiveX is a Microsoft technology that is designed to enable easier embedding of interactive objects, and often multimedia, on Web pages. ActiveX helps make Web pages more interactive, such as through animation or through the ability to open other applications in a browser (such as Microsoft Word or Adobe).

Besides enlivening Web pages, ActiveX technology can also execute programs, called ActiveX controls, on your computer via the Internet Explorer Web browser. ActiveX controls interact with the operating system just like any other executable software. ActiveX programs come with digital signatures from the program's author (that is, the company that created the program, not the actual software engineer). Think of a digital signature as being like a person's signature on paper. Your browser can look at a digital signature and see whether it is genuine so that you can know for sure who signed a program. You have two choices: either accept the program and let it do whatever it wants on your machine, or reject it. ActiveX security relies on you to make correct decisions about which programs to accept. Some ActiveX controls are harmless and improve your browsing experience, but malware writers can also create ActiveX controls to install unwanted programs on your computer. If you accept a malicious program, you're in big trouble.

You can adjust your Internet Explorer browser to prompt you when an ActiveX control wants to download to your computer. To find out how, see the section "Adjust Your Browser Settings."

Spyware and malware writers can also exploit software vulnerabilities in browsers (including alternative browsers such as Mozilla Firefox). Every software product in the world has defects that are discovered by researchers. Some of these researchers are security professionals; others are malicious attackers who use the discovery to attack the vulnerable software. Because Internet Explorer is the world's most widely used browser, it's a popular target for attackers. For instance, in June 2004 a Trojan horse called Download.ject emerged. Using a vulnerability in IE and IIS (Internet Information Server, which is Windows' Web server software), the Trojan horse installed itself on people's computers if they simply visited a Web site running on an infected Web server. Download.ject is an example of a drive-by download. Attacks that exploit software vulnerabilities are best dealt with by applying software fixes called patches, which are created and distributed by the software vendor. For instance, on the second Tuesday of every month, Microsoft releases the latest round of patches for its software. To download patches, go to http://windowsupdate.microsoft.com.

From Other Software

The most common method of spreading adware is to include it with other programs, such as file-sharing software or fun, cutesy utilities. Sometimes the provider of the software you want tells you that adware is also being installed. Sometimes it doesn't. In many cases, the software you want, such as a file-sharing

program, doesn't work if you disable the adware that comes with it. (See the later sidebar "Reading the Fine Print.")

From E-Mail

Spyware and Trojan horses may get onto your computer as e-mail attachments. For instance, many phishing attacks, in which a scam artist uses e-mail to trick you into revealing passwords, Social Security numbers, and other sensitive information, also includes malware such as keystroke loggers.

From Social Engineering

As discussed in Chapter 2, "Preventing Identity Theft," social engineering is a fancy way to describe a lie. Spyware and adware purveyors aren't above lying to get you to install software. The most common example of social engineering is to advertise a program or e-mail attachment as something that it isn't. A great example is the Naked Wife worm that showed up in 2001. It spread by e-mail and included an attachment that purported to be a naughty Flash movie. In fact, the attachment was a Trojan horse that would install itself on your computer, mail itself to everyone in your e-mail address book, and then start deleting files.

5.4 How to Protect Yourself from Spyware, Adware, and Trojan Horses

You can protect your computer from becoming infected with spyware, adware, and Trojan horses in a variety of ways. This section outlines several methods.

Use Anti-Spyware and Anti-Virus Software

The best way to protect yourself from spyware and Trojan horses is to use anti-spyware and anti-virus software. Both kinds of software can prevent known spyware and Trojan horses from being installed on your computer, and they may be able to prevent unknown malware as well.

Many anti-virus vendors now offer spyware and adware protection as part of a larger product suite that includes anti-virus software and a firewall. These suites are a great option because they are easier to manage than a handful of disparate stand-alone products. Also, you don't have to worry about Product A causing Product B to malfunction (or Products A and B together causing your computer to malfunction).

That said, you still may want additional protection from dedicated anti-spyware software. Why? The simplest reason is the defense-in-depth strategy (also known as the belt-and-suspenders approach); one product might catch spyware or adware that the other product misses.

So why not have two different anti-virus products as well? In fact, many corporations employ this very strategy: E-mail servers get loaded with anti-virus software from AV company number 1, while corporate desktops get anti-virus software from AV company number 2. However, consumers don't really need two different anti-virus products because, generally speaking, the AV vendors have established parity—each AV provider does about as good a job as the others.

That's not necessarily the case when it comes to spyware and adware. Security software companies are still struggling to define exactly what spyware and adware are. Each company has its own set of definitions, which means that each company identifies and deals with spyware and adware in slightly different ways. On top of that, spyware and adware writers have proven to be clever and innovative, and they are constantly finding new ways to burrow into your computer. New spyware and adware emerges at an incredible rate, and one company may have signatures before another company does, or one company may deploy a removal tool faster than another. The result is that Company A's anti-spyware protection may excel in some areas but stink in others, and vice versa for Company B.

You can purchase stand-alone anti-spyware software from a number of vendors, and you also have several good free options. So even if your AV software already scans for spyware, you might want to double-check it with another anti-spyware tool. Tables 5.3 and 5.4 list leading anti-spyware software, both paid and free versions.

That said, if you do run two separate anti-spyware programs, don't be surprised if they start causing problems. If that's the case, you have to decide which one you like better and abandon the other.

Top names in the anti-spyware market include Aluria Software which makes Spyware Eliminator; Sunbelt Software, which makes CounterSpy; Webroot Software, which makes Spy Sweeper; Lavasoft, which makes Ad-Aware; Tenebril, which makes SpyCatcher; and Computer Associates, which sells eTrust PestPatrol. Established anti-virus vendors also sell anti-spyware tools, and smaller vendors also offer decent products. Table 5.3 lists vendors. As of mid-2005, pricing ranges from $19.95 to $29.95 for standalone anti-spyware software, and $49.95 to $69.95 for security suites that include anti-spyware, anti-virus, a firewall, and

Table 5.3

Commercial Anti-Spyware Products

Product	Vendor	Web Site
ActiveScan Pro	Panda Software	www.pandasoftware.com
Ad-Aware SE Plus	Lavasoft	www.lavasoft.com
CounterSpy	Sunbelt Software	www.sunbeltsoftware.com
eTrust PestPatrol	Computer Associates	www.ca.com
F-Secure Anti-Spyware for Windows	F-Secure	www.f-secure.com
McAfee Antispyware	McAfee	www.mcafee.com
PC-cillin	Trend Micro	www.trendmicro.com
SpyCatcher	Tenebril	www.tenebril.com
Spy Sweeper	Webroot Software	www.webroot.com
Spyware Eliminator	Aluria Software	www.aluriasoftware.com
Symantec Norton Internet Security Spyware Edition	Symantec	www.symantec.com

other security products. Note that special offers and rebates may affect the final cost.

When choosing a product, look for a system that lets you conduct regular scans and perform real-time detection of potential spyware. Look for products that can detect and remove spyware and quarantine suspicious programs. (A quarantine function keeps the program from operating but does not remove it. Quarantining allows you to investigate whether a program should be removed.)

Like firewalls and AV products, anti-spyware products ask you to decide what to do with the programs they detect. Sometimes the decision is easy, but other times you may not be sure. Anti-spyware programs often provide information about the programs detected, but that information may be so technical that it doesn't help. Therefore, look for a product that includes significant information presented intelligibly to help you make that decision.

You also have to keep the software updated. Look for an interface that makes updates easy—or, better still, that automates the update process. Take advantage of free trials to test and see which interface you find the most useful.

To help you decide which product to choose, check out reviews from *PC Magazine* (www.pcmagazine.com), *PC World* (www.pcworld.com), and CNET (www.cnet.com), which regularly review and rate security products. You can also

check online forums for recommendations and reviews. Good forums are available at CastleCops (www.castlecops.com) and SpywareInfo (www.spywareinfo.com).

Beware of Opportunists

Anti-virus products have been around for years. In that time inferior or shady products have gone away, while at the same time a reputable group of companies have developed stable products that generally work as advertised. The anti-spyware market is in its infancy, and market forces that trim weak or disreputable businesses have yet to exert their full influence. Many products are rushed onto the market, and they just don't work very well. Some products also try to confuse users by taking names or registering Web sites that are similar to popular anti-spyware software. For instance, the name of a popular anti-browser-hijacking tool called HijackThis is often used by imitators or malware purveyors hoping to attract unsuspecting users to their own sites. The real HijackThis tool is available at www.merijn.org/downloads.html.

In addition, the opportunities presented by a hot new technology sector also attract those who aren't above unsavory (and illegal) tactics to convince you to buy their software. For instance, in March 2005 the FTC filed a complaint against a product called Spyware Assassin. According to the FTC, Spyware Assassin offered deceptive free scans that claimed to detect spyware on users' computers, even when no spyware was present. The scam even went as far as listing names and file locations of spyware on computers that were clean. Spyware Assassin then offered anti-spyware software (at $29.95 a pop), which the FTC says doesn't even work that well.

If you haven't specifically visited a site to request a scan, be suspicious of unsolicited and alarmist pop-ups that urge you to click or scan immediately—or that claim to have detected spyware on your computer without your having even requested a scan. As you would in the real world, be wary of such high-pressure sales tactics.

The vendors listed in this chapter are reputable, and you should feel comfortable doing business with them. If a vendor isn't listed here, that doesn't imply that its product is defective or misleading. That said, if you're dealing with a new or little-known company, be cautious. For instance, reputable companies always have a clearly posted EULA and privacy policy on their Web site. One way to check out a company is to search for the name and see what results come back. You can also post to an anti-spyware forum to get a sense of a company's reputation or to find out if others have had positive or negative experiences.

Free Anti-Spyware Software

The best thing about free anti-spyware software is that it's free! If you don't want to pay for anti-spyware software, these free options are absolutely recommended. They can also be used as a backup for paid software to ensure that your system is as clean as possible (or to check that your paid software is doing a good job). Note that if you use multiple anti-spyware tools, one may list the other as spyware. For instance, many anti-spyware programs list Spybot Search&Destroy, a free anti-spyware program, as spyware.

The downside of free software is that you may lose out on other benefits, such as help desk support. In addition, some free anti-spyware software is written and maintained by one person or a small group of volunteers, which means that they may be slower to provide new signatures, new features, and software fixes than commercial products. You may also have to seek out and manually download new updates, whereas commercial products usually offer automatic updates.

The two most popular free anti-spyware products are Lavasoft's and Spybot Search&Destroy. Lavasoft also sells a commercial version of Ad-Aware, but Spybot is free (although you can make donations to its creator if you find the tool useful). Lavasoft and Spybot Search&Destroy both offer forums where you can post questions and find new information about the software.

In January 2005, Microsoft released a free anti-spyware tool called, cleverly enough, Microsoft AntiSpyware. The underlying program was acquired from GIANT Software Company. The software includes both scanning and preemptive blocking capabilities. You can also participate in the SpyNet community, a forum for collecting and reporting information about unwanted software.

Another well-known free tool is an anti-spyware scanner built into the Yahoo! toolbar. The spyware capability is only one feature; others include a pop-up blocker and links to other Yahoo! sites. If you download the toolbar you can get access to an anti-spyware community where you can post to a message board and get information about new spyware threats. Note that the anti-spyware scanner in the Yahoo! toolbar is based on Computer Associates' eTrust PestPatrol software.

Finally, you can download two useful free tools—HijackThis and CWShredder. HijackThis provides a log of your Registry, which you can use to detect unwanted programs such as browser hijackers. CWShredder is a tool to remove CoolWebSearch adware, which is a family of some of the Internet's most virulent and persistent malware. InterMute, the company that offers CWShredder for free download, has been acquired by Trend Micro. At the time I wrote this

chapter, you could still find CWShredder at www.intermute.com/products/cwshredder.html. However, that may not be the case much longer. You may need to search www.trendmicro.com for the software, or download it from the Web site of Merijn Bellekom, who created CWShredder (and HijackThis). Table 5.4 lists this Web site and the sites of other free software.

What Anti-Spyware Software Can Do

Anti-spyware products scan your hard drive for unwanted software. When they detect that software, they ask you whether you want to delete it, quarantine it, or leave it alone. (Quarantining spyware leaves it on your computer but prevents it from operating.) Many products also perform proactive monitoring to ensure that unwanted programs aren't installed on your machine in the first place. For instance, Microsoft AntiSpyware includes components that monitor your applications and your computer's system settings in real time. It alerts you if attempts are made to change applications or settings. It also monitors programs on your computer that attempt to access the Internet.

Like the AV software discussed in Chapter 4, anti-spyware software uses signatures to detect malware on your computer. As you'll recall, a signature is

Table 5.4

Free Anti-Spyware Software

Product	Vendor	Web Site
Ad-Aware SE Personal	Lavasoft	www.lavasoft.com
HijackThis and CWShredder*	Merijn/InterMute	www.merijn.org/downloads.html (for HijackThis and CWShredder) http://www.intermute.com/products/cwshredder.html (for CWShredder)
Microsoft AntiSpyware	Microsoft	www.microsoft.com
Spybot Search&Destroy	Safer-Networking	www.safer-networking.org
Yahoo! Toolbar with Anti-Spy	Yahoo!	http://toolbar.yahoo.com/ie

**HijackThis and CWShredder are not full anti-spyware solutions. HijackThis is a tool for manually removing browser hijackers. CWShredder is a removal tool only for CoolWebSearch, which has spawned an entire family of spyware variants. Also note that Web sites for Merijn, Lavasoft, and Spybot are sometimes victims of Denial of Service attacks or other attempts to take them offline. If you find these Web sites unavailable, try again later.*

like a fingerprint of a specific piece of malware. Anti-spyware scans the files, registries, and programs on your hard drive, looking for these fingerprints. For anti-spyware software to be most effective, you must continually update the database of signatures. You must also scan your computer regularly to ensure that new spyware hasn't made its way to your computer. If you can, scan at least once a week.

You may also want to scan your computer before conducting sensitive transactions online, such as Web-based banking or other financial transactions. As discussed in Chapter 2, identity thieves try to plant spyware or Trojan horses on your computer to steal log-in information and passwords, or even piggyback on open sessions to make transactions of their own. You can feel more confident in your online transactions by running a scan first. Some companies have also started offering free malware scans to their customers before they engage in high-value transactions.

What Anti-Spyware Software Can't Do

Because anti-spyware software is signature-based, it requires a copy of known spyware to create a fingerprint. Like AV software, anti-spyware software is not guaranteed to prevent new spyware from infecting your computer.

Anti-spyware software does not offer complete protection from all classes of malware. While anti-spyware and AV products are beginning to overlap, anti-spyware software by itself is not sufficient protection from viruses, worms, and Trojan horses. In addition, anti-spyware products may not scan e-mail, which is becoming a popular infection vector for spyware. Deploy and run both AV and anti-spyware software for full protection.

Be Suspicious of Free Software

The Internet is crawling with free software, including games, file-sharing programs, screen savers, and so on. Some of it is quite harmless, and some of it is not. Companies often offer "free" software that includes adware or spyware. You should be suspicious of offers of free software. If the software doesn't include a EULA, privacy statement, and clear instructions on how to remove the software later, you may want to avoid downloading it.

Read the EULA

The End User License Agreement (EULA) is a contract between you and the software vendor. When you download and install software, you are presented with a screen that includes the EULA. The software does not allow you to continue installation until you click a button acknowledging that you've read and agreed to the terms of the agreement. Most people simply click the button without reading the license.

This is a mistake, especially with free software, because it often includes adware or other unwanted programs. Legitimate companies that offer free software inform you of the presence of adware somewhere in the EULA (probably toward the end) and give you the option of refusing the entire package. If you understand that accepting the free software means accepting the adware as well, you should proceed with the download.

If you've read the EULA and you found no mention of programs or functions that monitor your computer use, and then later you discover that the software did include unwanted programs, you can report the software provider to the FTC. The FTC is empowered to take action against companies that engage in deceptive practices. See the "Helpful Resources" section near the end of this chapter for information about filing complaints.

Adjust Your Browser Settings

You can adjust the IE browser's settings so that it warns you when an ActiveX control wants to be downloaded and so that it lets you accept or deny the download. To check the setting, open IE and select Tools and then Internet Options, and then click the Security tab. You see four Web zones for which you can adjust security settings: Internet, Local intranet, Trusted sites, and Restricted sites, as shown in Figure 5.4.

To change the settings for each zone, click the zone icon you want to adjust, and then click the Custom Level button. A new window called Security Settings opens, as shown in Figure 5.5. You can set individual rules for dealing with ActiveX controls, or simply choose the Medium setting near the bottom of the dialog box. As long as you've set the IE Security setting to Medium, you get a warning message; any other setting allows ActiveX controls to download without notification. (As mentioned, browser security is covered in greater detail in Chapter 7.)

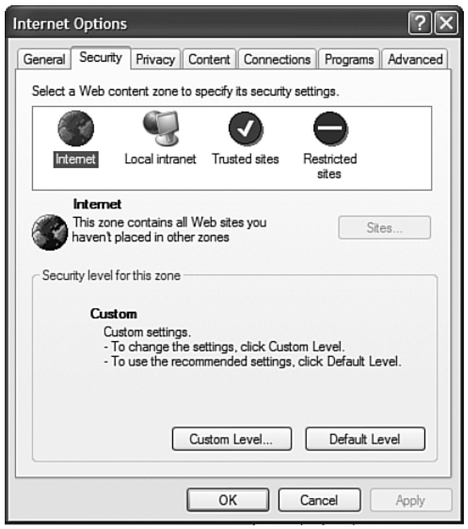

Figure 5.4 Internet Security options.

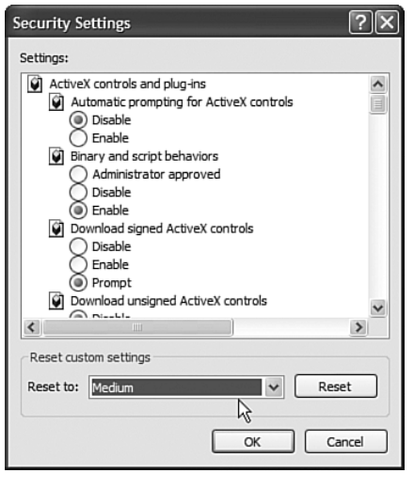

Figure 5.5 The Security Settings dialog box.

Unfortunately, even if a dialog box pops up to alert you of a download, clicking No doesn't always help. Some malware writers manipulate the dialog box so that clicking No or any other button still downloads the software. Attackers may

also try to disguise these pop-up messages to look like messages from your Windows PC as opposed to an ActiveX control, or make them appear to be generated by the Web site you're visiting. These messages are usually alarmist and prompt you to take some action immediately, such as clicking the Yes button to run a scan or download a program to repair the "problem." You should ignore these messages.

To close dialog boxes and pop-ups without clicking the No or Cancel button or the X in the upper-right corner, you can press Alt-F4. This safely closes windows inside a browser without allowing any downloads.

Use an Alternative Browser

Another option to help prevent spyware from being downloaded to your computer is to use a browser other than Internet Explorer. For instance, the Firefox and Opera browsers don't use ActiveX, which prevents ActiveX-based exploits from affecting your computer. These browsers are also less frequently subjected to vulnerability exploits (in part because they aren't nearly as widely used as Internet Explorer, and malware writers typically go after the most-used applications to infect as large an audience as possible). That said, alternative browsers are not invulnerable. (For example, from July to December 2004, there were 21 vulnerabilities affecting Mozilla browsers compared to 13 vulnerabilities affecting Microsoft Internet Explorer.) Therefore, if you do use one, you should check regularly for updates. You may also find that some Web sites don't work as well with alternative browsers.

To download the Firefox Web browser, go to www.mozilla.org. To download the Opera browser, go to www.opera.com.

Keep Your Software Updated

Updating your software is the computer equivalent of eating your vegetables: It is essential for good health, and you have to do it regularly. New spyware and adware programs are created all the time, as are the new signatures to detect them. Thus, it is important to update your security software. Most programs allow updates to be delivered automatically to you over the Internet.

The same applies for your operating system and application software. As noted earlier, Microsoft releases new updates, also called patches, on the second Tuesday of every month. Chapter 7 tells you how to set up your computer to get Microsoft updates automatically. Other vendors also release new software updates

to address vulnerabilities that might allow an attacker to harm or commandeer your computer.

5.5 How to Remove Spyware, Adware, and Trojan Horses

If you follow all the preventative steps described here, you can keep most spyware and Trojan horses off your machine. But it's still possible that some program somewhere will slip past your defenses, so it's important to know the signs of infection and how to remove the unwanted software.

Your best bet for getting rid of unwanted software is to use anti-spyware and anti-virus tools. These tools search your computer for any traces of known spyware, adware, and Trojan horses. Once these traces are found, you can choose whether to delete, disable, or leave the programs alone. You can also remove spyware and Trojan horses manually, using tools available on the Internet.

How to Tell if Your Computer Is Infected

As with viruses and worms, the best way to tell if you've been infected with spyware, adware, or a Trojan horse is to use anti-spyware and anti-virus software. These programs detect the presence of unwanted software on your machine and provide you with options for dealing with it. You should regularly scan your computer with both kinds of software and also make sure that your security software is running while you surf the Internet.

If you don't already own anti-spyware software, you can get free scans from a variety of anti-spyware vendors. Webroot Software offers a free scan called Spy Audit, which can be found on the company's home page at www.webroot.com. Zone Labs at www.zonelabs.com, and Symantec at www.symantec.com, also offer spyware scans. Computer Associates offers a free scan at www.ca.com. Click the Products link under the Home and Home Office listing, and then click eTrust PestPatrol. That takes you to the page to run the scan. You can also get a free scan from Aluria Software by surfing to www.aluriasoftware.com. Many of these scans use an ActiveX control, so you have to click through a warning screen in your Internet Explorer browser.

You can also look for the following signs:

- Is your computer deluged with advertising?
- Does your Web home page keep changing even if you change it back?

- Are you directed to unfamiliar search sites that you didn't request?
- Is your computer sluggish, particularly when Web surfing? Spyware and adware that keep track of your activities use your Internet connection to send reports and direct advertising to your computer. This behavior steals bandwidth and affects the speed at which Web content gets delivered. Spyware and adware also use your computer's Central Processing Unit (CPU). If enough adware or spyware gets on your machine, this software competes for processing power with other applications and affects the overall speed at which your computer performs normal functions. In many cases, infected computers simply become inoperable.
- Does your computer crash frequently?
- Do ads pop up on your computer even if you're not on the Internet?
- Do you see a new toolbar in your Web browser?
- Have you or someone who uses your computer downloaded "free" programs such as file-sharing software, weather trackers, screen savers, or utilities that claim to enhance your online experience?
- Does your firewall detect programs on your computer trying to access the Internet?

Using HijackThis

To manually remove unwanted programs from your computer, you have to delete the files and Registry entries these programs create. This requires you to know what changes the spyware made to existing Registry keys and which new Registry keys it installed.

A popular tool for removing browser hijackers from the Registry is HijackThis. It scans your Registry and gives you a list (called a log) of the contents. You can then choose which of the contents to remove. You can find a copy of HijackThis at its creator's site: www.merijn.org/downloads.html. (He is also the creator of CWShredder, a popular removal tool for CoolWebSearch. CoolWebSearch is one of the most persistent and fast-evolving pieces of spyware on the Internet. CWShredder is available for free at www.merijn.org/downloads.html.)

> HijackThis is a manual tool, meaning you have to remove unwanted content yourself. Unlike most commercial anti-spyware software, HijackThis doesn't offer advice on what you should and shouldn't remove. It is highly recommended that you get help in deciding which parts of the Registry to remove. If you make mistakes when changing your Registry, your computer may not work correctly. If you have a support contract with an AV or anti-spyware company or with your computer manufacturer, they may help you with a HijackThis log.

Alternatively, you can get free help with your HijackThis log at a number of online forums. These online forums are run by knowledgeable users who can help you review your log and make changes. One popular forum is CastleCops. Go to www.castlecops.com and click the Forums button near the top of the page, and then scroll down to the Privacy section and click the HijackThis - Spyware, Viruses, Worms, Trojans Oh My! entry, as shown in Figure 5.6. Be sure to read the guidelines for using the forum and posting HijackThis logs. CastleCops also has a technical tutorial on HijackThis at http://castlecops.com/HijackThis.html.

Figure 5.6 CastleCops' HijackThis Forum.

Another option is SpywareInfo, at www.spywareinfo.com. On the home page you can scroll down to look for a section called The Browser Hijacker Articles. The links in this section provide information on how to use HijackThis. You can also register to post your log or questions at a user forum. It also provides links to other online forums where you can review your HijackThis log.

You can also post logs at Spyware Warrior (www.spywarewarrior.com). Further listings to get assistance with HijackThis logs are at www.merijn.org.

Reformatting Your Hard Drive

In the worst-case scenario, the anti-spyware software won't be able to remove the unwanted programs, and you'll need to seek outside help. If you've purchased anti-spyware software, contact customer support to see what they recommend (but be prepared for a long wait). You can also contact your computer's manufacturer, seek help from the store where you bought the computer (for a fee, of course), or contact a local computer repair shop.

As a last resort, you might have to start from scratch and simply reinstall the operating system and applications using the original software discs. To do this, simply insert the original operating system disc into your CD drive and start the computer. The computer prompts you to reconfirm that you want to reinstall the operating system. However, reinstalling the operating system erases all the data you've saved on your computer (let's hope you have good backup habits). This is a last-ditch effort: exhaust other options before reformatting your hard drive.

5.6 Checklist

Use this checklist as a quick-reference guide to the material covered in this chapter.

Do

- Use anti-spyware software, and keep it updated.
- Adjust your browser settings to be notified of ActiveX downloads.
- Read the EULA before you download any software.
- Be suspicious of free software.
- Keep your application and operating system software updated.
- Perform regular backups of essential files.

Don't

- Accept unsolicited software downloads.
- Click pop-up ads or unsolicited and alarmist pop-ups that claim you have spyware or other problems with your PC.
- Accept e-mail attachments from strangers.

- Open e-mail that claims to come from a financial institution or e-commerce site that you don't do business with.
- Accept software without reading the EULA.
- Be afraid to try a new Web browser.

5.7 Helpful Resources

This section presents additional resources to help you learn more.

Ben Edelman is a law student at Harvard University and an anti-spyware researcher. His Web site is loaded with great information about deceptive practices of adware vendors, how programs exploit security holes, and critiques of anti-spyware legislation. You can read his postings at www.benedelman.org.

Spyware Warrior is an informative site about all things spyware, run by Eric Howes. If you're looking for a spyware product, check out the link that compares various anti-spyware software, including free products. The link to the Spyware blog takes you to a Web log with lots of current information about new spyware and developments in the anti-spyware community. You can also join various forums and post HijackThis logs. Go to www.spyware.com.

PC Pitstop offers diagnostic tools for PCs and also provides useful information about spyware. For instance, check out its ranking of the top 25 spyware and adware programs at http://www.pcpitstop.com/spycheck/top25.asp.

Merijn Bellekom is the author of HijackThis, CWShredder, and other useful anti-spyware tools, all of which you can download at www.merijn.org.

Spywareinfo.com is chock full of good information. If you'd like to learn more about spyware, cookies, browser hijacking, and more, click the More Links button on the opening page. It also recommends products to help you deal with unwanted software. If you register at the site, you can post questions to a message board and get assistance with spyware problems (just be sure to read the FAQ first). You can also subscribe to the newsletter, written by Mike Healan, the site's creator.

To read a copy of the FTC's March 2005 report on spyware, go to www.ftc.gov/os/2005/03/050307spywarerpt.pdf. To file a compliant about spyware or adware with the FTC, go to www.ftc.gov and click the File a Complaint link on the opening page. You can also call 877-FTC-HELP (877-382-4357).

Spywareguide.com has a searchable database of known spyware and adware. You can enter a program's name into the search bar on the home page to see if the program is listed. The site also ranks spyware programs according to a danger level of 1 through 10, with descriptions of each level.

Reading the Fine Print

Kazaa, which makes peer-to-peer software for sharing files over the Internet, includes adware in the free version of its product. Of course, the software is free because you agree to have adware generate targeted advertising.

The company explains this in its EULA, which you can read at www.kazaa.com/us/terms2.htm. The sections on adware are listed toward the bottom of the EULA in Section 9. As of mid-2005, Kazaa bundled five adware programs, including Cydoor, an advertising delivery program that, according to the Kazaa EULA, "uses your Internet connection to update its selection of available ads and stores them on your hard drive."

It also includes the GAIN AdServer, which, according to the Kazaa EULA, "identifies your interests based on some of your computer usage and uses that information to deliver advertising messages to you."

The Kazaa EULA also includes links to the EULAs for Cydoor and GAIN AdServer and says that by downloading Kazaa you basically acknowledge and accept the EULAs for each of these software components.

In addition, the EULA states that you will not use any other software to disable or block any of the ads that are served by these components. If you remove any of these components, Kazaa ceases to function.

So what should you do if you really want the free file-sharing software? You have to decide about the trade-offs. As long as you're willing to accept the consequences that come with adware (annoying ads, potentially poorer performance on your PC, and whatever vulnerabilities are introduced by having adware on your computer), you can download the software and start sharing files.