CHAPTER 5

Tip 5: Lock Out Spyware and Adware

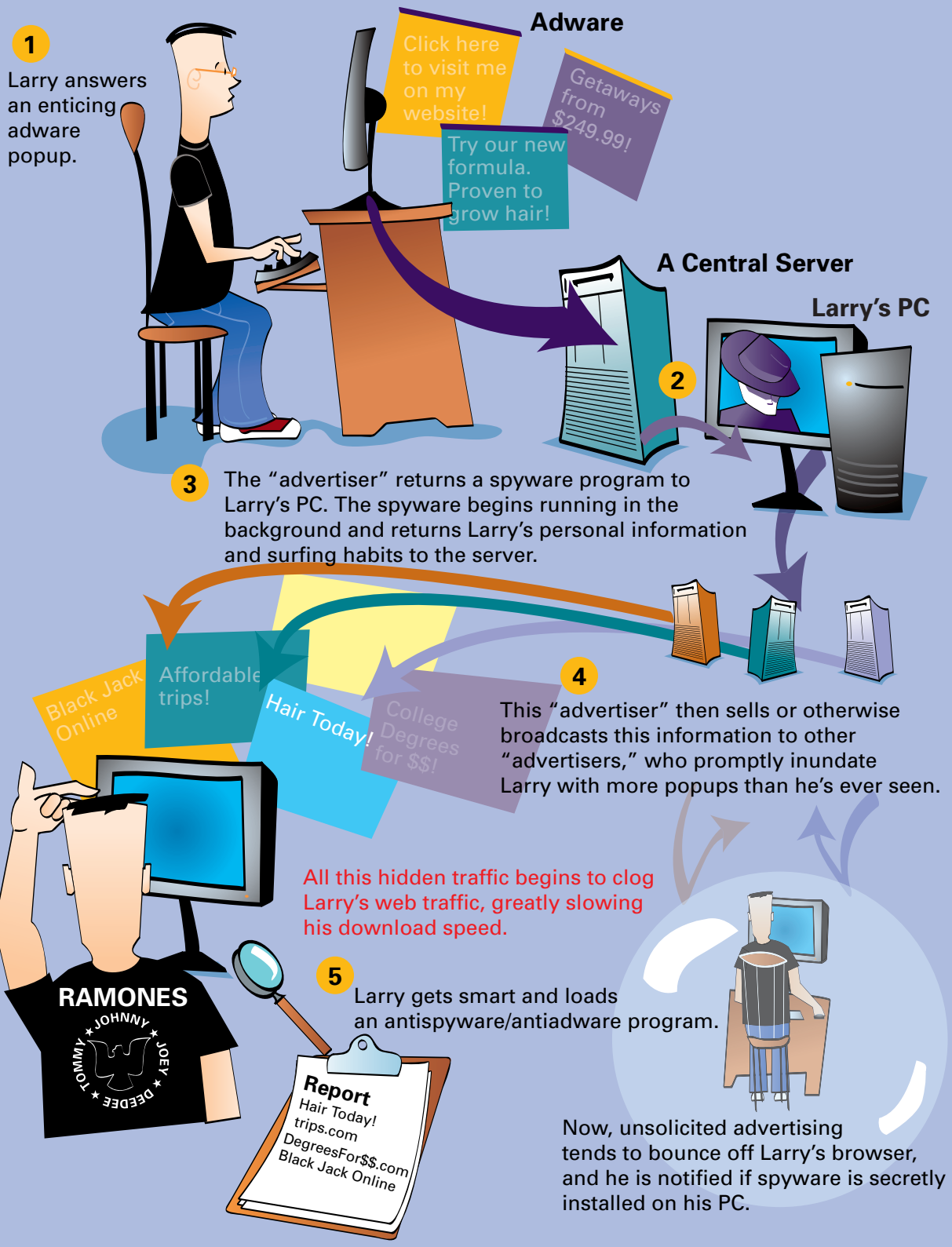
Threat Type: Software based, victim enabled

Examples of Threats:

- Popping up advertisements all over your computer screen
- Installing programs to collect and report data on your Internet browsing habits
- Inserting toolbar or searchbar programs into your browser or applications, such as Internet Explorer, which slow down your computer's performance
- Collecting and reporting information about which websites you visit so that you can be targeted more effectively with advertisements and marketing

Our Tips:

- Install and enable a popup blocker.
- Install and enable a spyware/adware blocker.
- Use a personal firewall program on each computer to prevent unauthorized program installations and Internet access (see Chapter 1, "Tip 1: Use Firewalls").
- Avoid downloading "free" software programs that have strings attached.
- Periodically use a spyware elimination program to find and delete spyware and adware.


1
Larry answers an enticing adware popup.
Adware
Click here to visit me on my website!
Getaways from $249.99!
Try our new formula. Proven to grow hair!
A Central Server
Larry's PC
2
3
The "advertiser" returns a spyware program to Larry's PC. The spyware begins running in the background and returns Larry's personal information and surfing habits to the server.
Black Jack Online
Affordable trips!
Hair Today!
College Degrees for $$!
4
This "advertiser" then sells or otherwise broadcasts this information to other "advertisers," who promptly inundate Larry with more popups than he's ever seen.
All this hidden traffic begins to clog Larry's web traffic, greatly slowing his download speed.
RAMONES
JOHNNY
JOEY
DEEDEE
TOMMY
5
Larry gets smart and loads an antispyware/antiadware program.
Report
Hair Today!
trips.com
DegreesFor$$.com
Black Jack Online
Now, unsolicited advertising tends to bounce off Larry's browser, and he is notified if spyware is secretly installed on his PC.

One of the engines that has driven the explosive growth of the Internet is the concept of eyeballs. For a relatively low price, you are provided with a high-speed broadband connection that gives you access to an endless amount of mostly free information, services, digital media, and even software programs.

Ever ask yourself how these companies stay in business? For example, how does Weather.com pay their bills to be able to bring you awesome up-to-the-minute radar images for your city's weather? How can people give you software programs such as screensavers and games for free?

The answer is eyeballs. *Eyeballs* refers to the number of people's eyes someone can get to view their Internet content (and accompanying advertisements). Yes, the Internet is based on relatively the same concept as commercial television.

The difference is the Internet can bring highly targeted advertising like never before and sometimes nearly force you to view it. Banner and popup ads were the first wave, but most people are tuning them out, so to speak, by installing popup blockers. So, advertisers are relying on more sophisticated methods to get their stuff in front of your eyes.

An all-out brawl is looming between consumers and advertisers. Between cable networks, DVRs, and TiVo players, we can screen out quite a few commercials. With increasingly good technology, we can also screen out a lot of advertisements online, too, which is the focus of the rest of this chapter.

What Is Spyware and Adware?

So, why spyware and adware? Well, quite frankly, online advertisers are getting more desperate to keep the ads under your nose. As a result, there is an escalation of techniques occurring, some getting pretty aggressive. These techniques include adware and spyware.

Adware

There is not one agreed upon definition of what *adware* is and is not, but in general it includes any program used to facilitate getting advertising content in front of you on your computer, including the following:

- **Popups**—Advertisements that pop up on your computer screen as new windows, especially while you are browsing the Internet.
- **Adware**—Although the whole category of advertisements is often referred to as adware, the term also is used in reference to hidden programs inside of other programs. This is usually from free software or a game you download that is permitted to shower you with ads as the price you pay for using it for free.
- **Annoyware**—Term for aggressive adware practices, such as asking whether you want to install a program and then only allowing you to click OK and not Cancel, or popups that when you close them keep popping up more and more additional ones.
- **Banner ads**—Blending an advertisement into a website in an official-looking banner, enticing you to click it because you think it is part of the page you are browsing.

- **Drive-by downloads**—Suddenly asking you to download a program that you did not ask for while browsing the Internet.
- **Warning boxes**—Making a popup ad look like a typical warning box you get in Windows. Our favorites are those that claim your system is infected with adware/spyware and then try to sell you an antiadware program. Adware selling antiadware. Beautiful.

Most adware is obtained willingly, by you agreeing to see advertisements for using a free piece of software or service on a website. You probably do not even notice this in the fine print of the user agreement when you click the Accept button. (Adware vendors are counting on the fact that you don't.)

Spyware

There is also not one agreed upon definition of what *spyware* is and is not, but in general it includes any program used to gather and relay information from your computer to a location collecting the information, including the following:

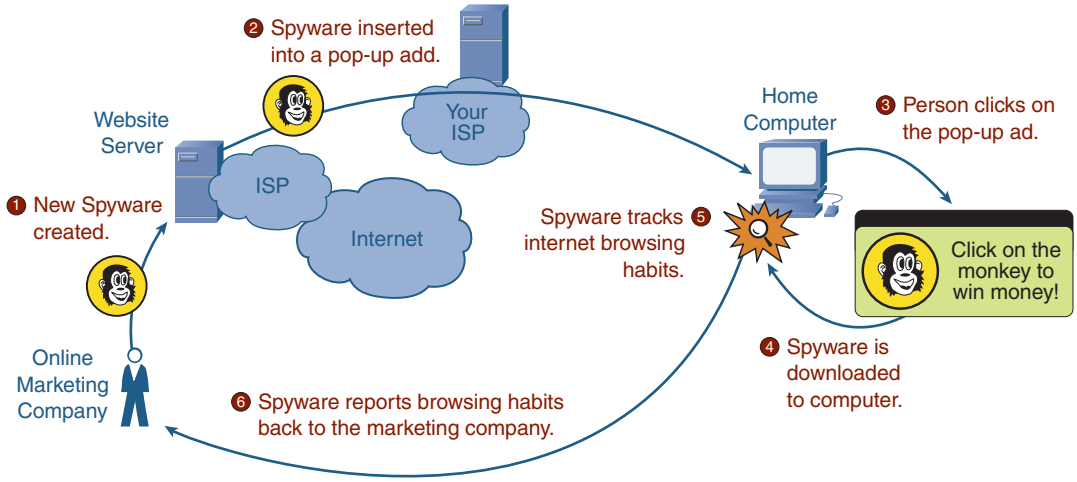
- **Data miners**—Actively collect information from you and then relay it to a remote server.
- **Spyware**—As in the adware case, this term is used for both the category and for a particular instance within the category. In this case, we are referring to a hidden program that collects information and sends it to a central server without your knowledge or consent.
- **Trackware**—Generally passive method of tracking with cookies what site or sites you have visited and also some amount of personal information.
- **Hijacker**—These little gems like to hijack your Internet Explorer settings, such as changing your home page to where they want you to go or hijacking and overlaying the search function.
- **Searchbars and toolbars**—Toolbars for searching that can be added as add-ons to Internet Explorer. They generally cause slow performance on your computer and can be used to track what information you search for and browse.

Some spyware is obtained willingly, by you agreeing to participate in some trial marketing for using a free piece of software or service on a website. Just as often, you might think you are agreeing to adware when in reality a program has been placed on your computer that can collect information and send it to a marketing company.

Figure 5-1 shows an example of spyware. In this example, the spyware program is put in a popup ad as a payload. When the computer user clicks the popup ad, the spyware program is deposited on the computer.

After the initial deposit, the spyware can track whatever it was created for (for example, which applications are running on the PC or which web pages are browsed most often). Periodically, the spyware can call home, by sending its information to the creating company over the Internet.

Figure 5-1 How Spyware Works



Are Spyware and Adware Viruses?

Although many adware and spyware programs increasingly share some of the characteristics of viruses, especially stealth and doing things without your knowledge, the primary distinction is that viruses live to replicate, whereas spyware and adware live to gather information that can be sent to marketing companies or to entice you to buy a specific product.

In general, spyware and adware are a one-to-one relationship between you and whatever marketing organization is trying to sell you stuff. They generally do not replicate themselves and send themselves to other computers. Spyware and adware tend to operate more on the "cow pattie" model: meaning they lie around on websites until you step in one, and then they cling to your shoe until you can shake them loose.

Preventing Spyware and Adware

Adware is mainly an annoyance but can slow down the performance of you computer. Spyware is a larger threat because it can be an invasion of your privacy. You can take four steps to remedy the threat:

- Exercise common sense.
- Block popups.
- Install an antispyware/antiadware program.
- Implement a personal software firewall.

The first three are covered in the sections that follow. Personal software firewalls are covered in Chapter 1.

Exercising Common Sense

The easiest way to avoid dealing with spyware and adware on your computer is the same as for viruses: Do not get them in the first place. Easier said than done, but here are some tips:

- Avoid downloading "free" software programs, screensavers, and any program that comes with strings attached.
- If you are not sure whether there are strings attached, do some quick Internet research on the software program.
- Do not click on popup ads, even to win money from a monkey.
- Do not fall for popups on your computer saying your computer is infected with spyware.
- Ask yourself why something of value is being offered for free. What do they have to gain from giving it to you?

It is almost impossible never to get adware or spyware on your computer. Just like viruses, we have had them, and everyone we know has had them.

Installing a Popup Blocker

The first step in avoiding adware and spyware (and to save yourself a ton of annoyance) is to turn on a popup blocker to stop the endless stream of windows with advertisements popping up on your computer screen while you are on the Internet. You have a couple of options.

Turning On the Internet Explorer Built-In Popup Blocker

If you are running Windows XP Service Pack 2 (SP2), you have a popup blocker already. All you need to do is turn it on. If your version of XP is not SP2, you can acquire it here:

http://www.microsoft.com/windowsxp/sp2/default.mspx

The popup blocker is built in to Internet Explorer. To turn it on, click **Tools > Pop-up Blocker > Turn On Pop-up Blocker**, as shown in Figure 5-2.

That was easy. Periodically, some websites might use popups you want to see, not as ads but as part of the way that website functions to show you information. You can just toggle the popup blocker in your browser off temporarily. Just remember to turn it back on when you leave that website.

When you turn on the popup blocker, the menu option will change to **Tools > Pop-up Blocker > Turn Off Pop-up Blocker**. You just use the same menu option to toggle the feature on and off.

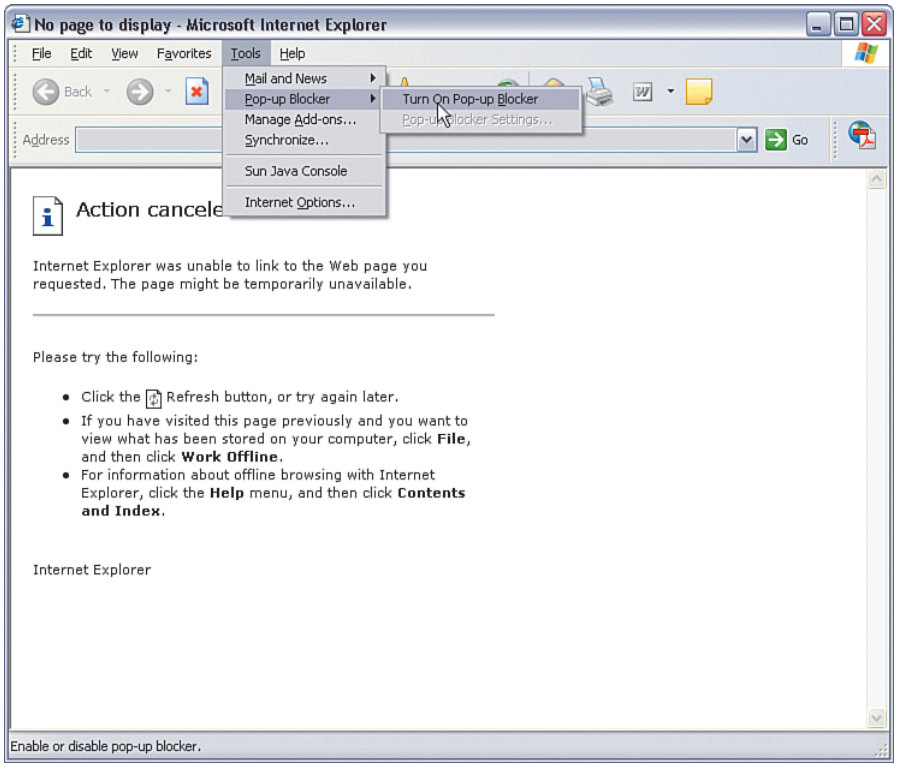
Installing a Third-Party Popup Blocker Program

If you do not have Windows XP (still running Windows 98SE, 2000, or ME), you do not have the option to upgrade Internet Explorer to receive the built-in popup blocker.

However, several popup blockers are available for free (yes, we know we said not to download free stuff). Pop-Up Stopper from Panicware is a pretty decent one. You can get it here:

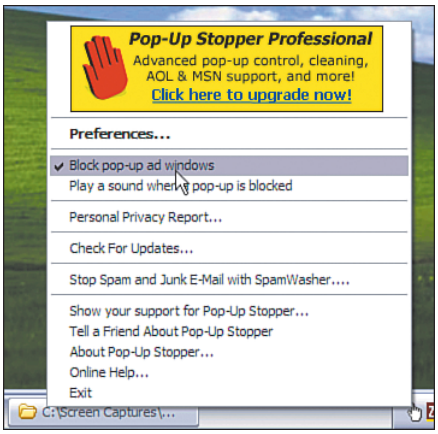
http://www.panicware.com/product_psfree.html

Figure 5-2 Enabling the Internet Explorer Popup Blocker



After you install it, a little white glove icon will appear in the lower right of your screen (on the running tasks bar). If you double-click the glove, you can toggle Pop-Up Stopper on and off, as shown in Figure 5-3.

Figure 5-3 Panicware Pop-Up Stopper

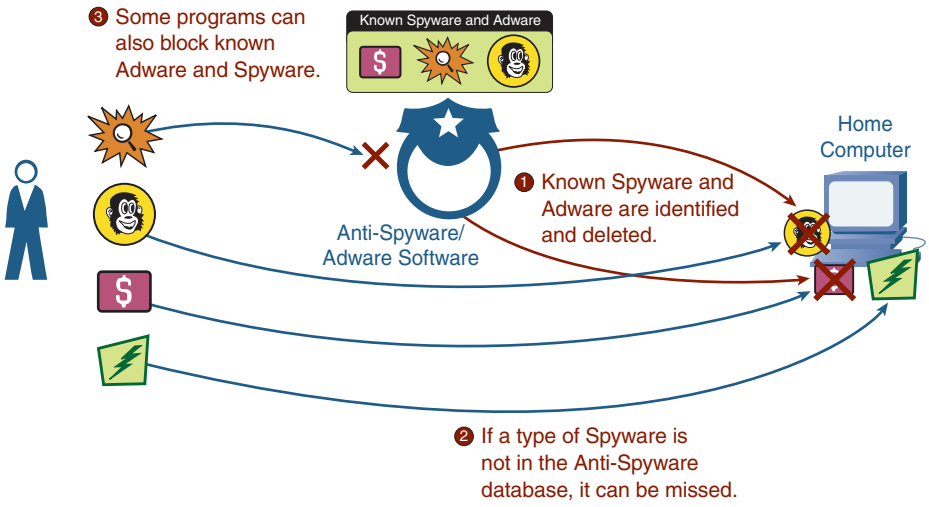


If the glove is white, Pop-Up Stopper is on. If the glove is "empty" (no color), Pop-Up Stopper is off.

Installing an Antispyware/Antiadware Program

The next step in adware and spyware prevention is to install an antispyware/antiadware program. Figure 5-4 shows how these programs work. They work similarly to antivirus programs.

Figure 5-4 How Antispyware/Antiadware Works



Your computer is scanned for known spyware and adware programs, matching them against a list of known spyware/adware signatures. If detected, you can remove them. If a piece of spyware is not yet in the signature list, it will be missed, again similar to antivirus.

Also similar to antivirus, but not quite there yet in terms of technology (that is, it is pretty new at the time of publication), is the ability to do active scanning, meaning blocking the insertion of adware and spyware into your computer in the first place. This is preferable rather than detecting and deleting it, after it is already on your computer and operating.

You have several options for antispyware/antiadware programs, including the following:

- Installing a freeware program from the Internet
- Installing Windows Defender, a relatively new option
- Enabling the antispyware/antiadware function in a security bundle you already own or plan to buy

The following sections look at each option. Any option will work, but they do have different advantages and disadvantages, so weigh which one is right for you. You might want to install all of them and then pick which one is right for you. Multiple programs for scanning are okay. However, be careful having multiple programs setup for active scanning at the same time because it could affect your computer's performance.

Free Antispyware/Antiadware Programs

A couple of really good antispyware/antiadware programs are available on the Internet for free. If you have been paying attention at all, you should be saying, "Hey, you told me not to do that." Well, exceptions apply to every rule.

The basic version of these programs is free. They make money by offering an upgrade to a premium version that has more features and a higher level of service. We look at the basic versions here.

Spybot Search & Destroy

The first is a product called Spybot Search & Destroy from Safer Networking. It is available here for download:

http://www.safer-networking.org/

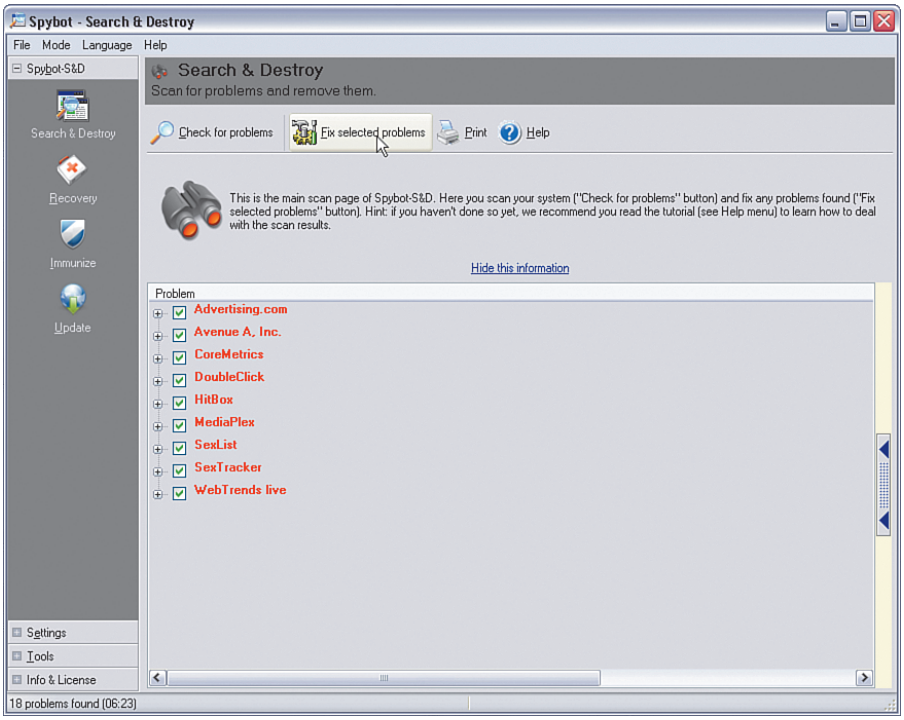
After installing the program, you can double-click the desktop icon to start it. You will see a dialog like Figure 5-5.

Figure 5-5 Spybot Search & Destroy Main Control Panel

Clicking **Search for Updates** downloads the latest signatures over the Internet to your computer so that Spybot has the latest set of spyware/adware knowledge to search with.

Clicking **Check for problems** scans your computer for known spyware and adware problems. When the scan has completed, you will see a display such as Figure 5-6, showing the spyware and adware programs that were detected on your computer.

Figure 5-6 Spybot Scan Completed and Spyware/Adware Detected



Clicking **Fix selected problems** removes all the spyware and adware programs that are checked.

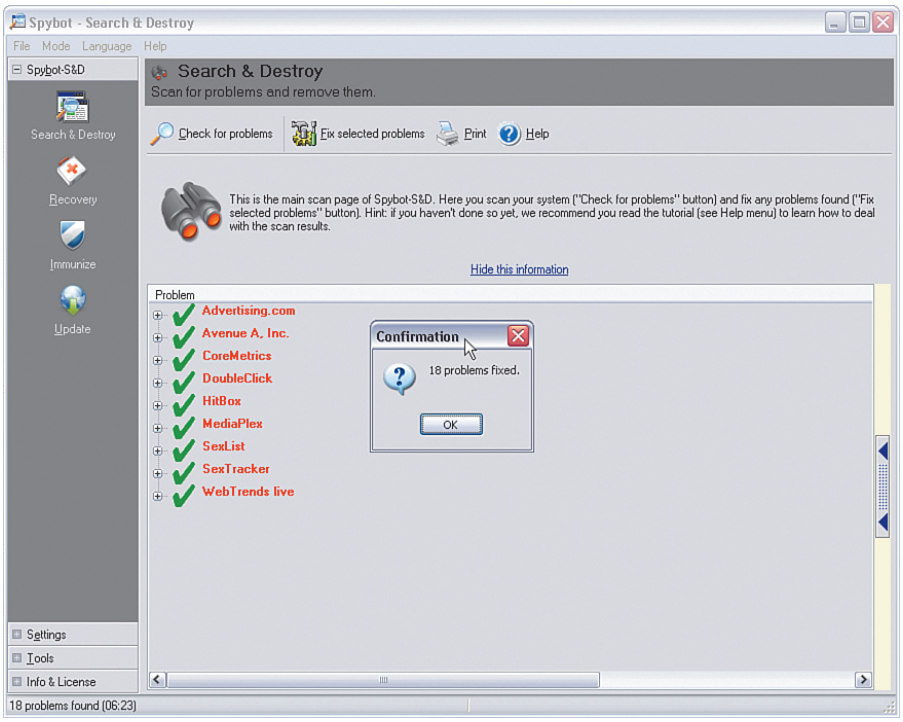
VERY IMPORTANT: Some adware programs are on your computer because you downloaded something, such as a screensaver program, that you are using for free under the agreement that the adware can live on your computer and bring you advertisements. If you remove the adware with Spybot or any other tool, you will likely disrupt the freebie program you are using. So, if you want to keep a particular piece of adware, uncheck it in the list before you click Fix selected problems.

Spybot attempts to remove the selected adware and spyware programs and gives you a report about whether it succeeded, as shown in Figure 5-7.

That's it, pretty easy, but you do have to remember to perform a scan periodically.

VERY IMPORTANT: Adware and spyware scans have to search a lot of files on your hard disk; so, depending how large your disk is, how many files you have, how fast your computer is, and how many adware and spyware signatures the program needs to look for, it can take several minutes to complete a scan.

Figure 5-7 Spybot Removes Spyware/Adware



If you would rather automate when scans occur, you can do that, too. Follow these steps:

Step 1 Click the **Mode > Advanced** option on the toolbar to turn on the more advanced functions of Spybot Search & Destroy.

Step 2 Click the **Settings** plus sign on the left side of the control window. Then, click **Settings** below that. Page down in the panel on the right of the window to a section called Automation, as shown in Figure 5-8.

Step 3 Under System start, select the following options:

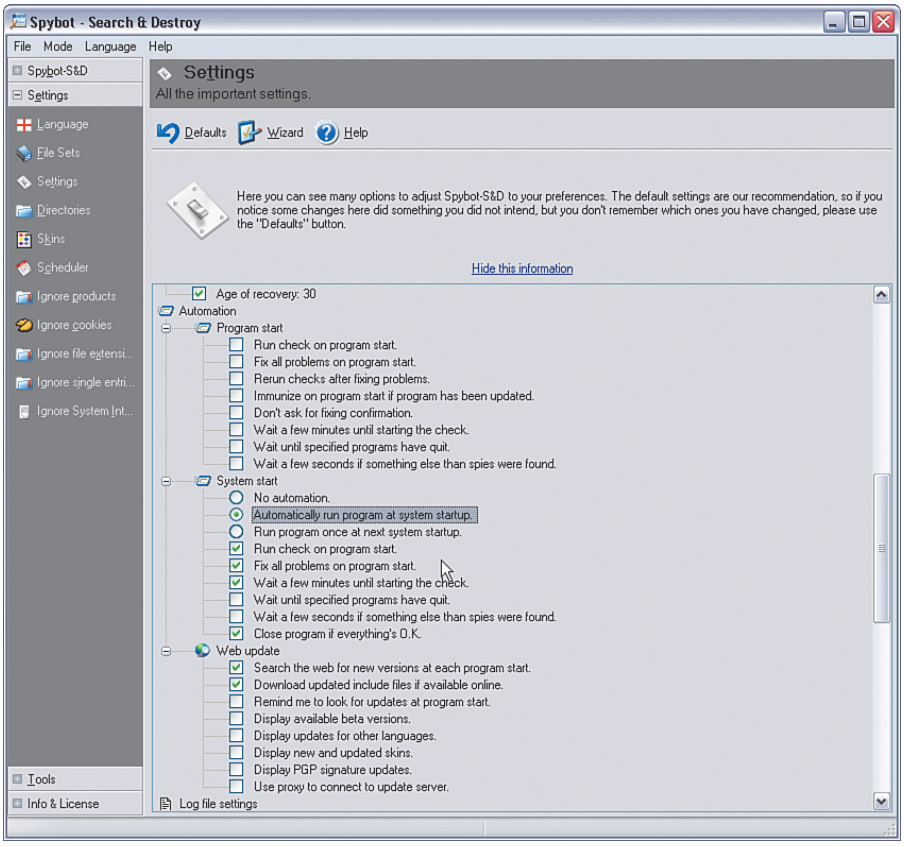
- **Automatically run program at system startup.**
- **Run check on program start.**
- **Fix all problems on program start.**
- **Wait a few minutes until starting the check.**
- **Close program if everything's O.K.**

Step 4 Under Web update, select the following options:

- **Search the web for new versions at each program start.**
- **Download updated include files if available online.**

Step 5 Click **File > Exit** to save the settings.

Figure 5-8 Spybot Settings for Automated Scanning



Now, each time Windows is started, Spybot will automatically start, download the latest adware/spyware signatures, and start scanning. The scanning looks slightly different, as shown in Figure 5-9. Because many different programs compete for the CPU resources as the computer starts up, it is a good idea to set the startup time to about 4 or 5 minutes after Windows boots.

Figure 5-9 Spybot Auto-Scanning After Windows Boot

When the scan completes, Spybot automatically removes any detected spyware and adware.

Spybot Search & Destroy is a pretty good antispyware/antiadware program. It is mainly a "sweeper," meaning it scans and removes spyware programs after they are already there. A few prevention features are starting to appear in Spybot. Check out the Immunize function.

Finally, the good folks at Safer Networking operate today based on donations. So, if you like Spybot Search & Destroy, consider kicking a few euros their way (they are based in Ireland).

Ad-Aware

The next product to consider is called Ad-Aware from Lavasoft (a Swedish company; apparently Europeans hate adware and spyware even more than Americans).

It is fairly similar to Spybot, in that it is a "sweeper" type of program. The basic (personal) version is free, with a more enhanced version available for a small fee. One of the features available in the pay version is Ad-Watch, which offers spyware/adware prevention and blocking before it reaches your computer. Both versions are available here:

http://www.lavasoft.com/

After you have installed Ad-Aware, you can access the Ad-Aware main control window by double-clicking the desktop icon. It looks like Figure 5-10.

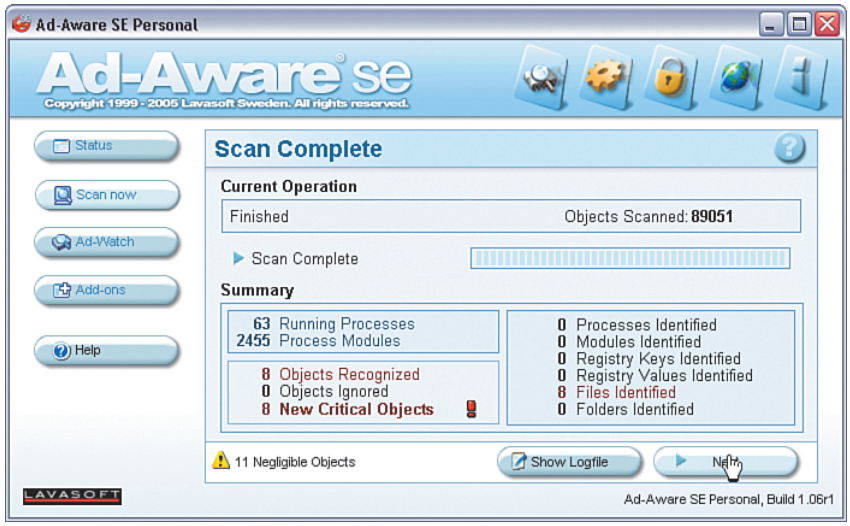
Figure 5-10 Ad-Aware Main Control Window

Clicking **Check for updates now** checks for and downloads the latest signatures from the web. Clicking **Scan now** triggers a full system scan against the known adware and spyware signatures. When it completes, you receive a report like that shown in Figure 5-11.

To remove any detected items, click **Next** and follow the instructions.

Ad-Aware is another pretty good product. If you try it and like it, consider upgrading to the pay version to get the prevention component, Ad-Watch.

Figure 5-11 Ad-Aware Scan Completed and Spyware/Adware Detected



Windows Defender

The next option to consider is called Windows Defender (beta 2), formerly known as Windows AntiSpyware (beta). Defender is a beta version (at the time of this writing) of antispyware/antiadware from Microsoft that integrates with Windows. (Beta means it is still undergoing testing, but you can use it at your own risk.)

Defender can run on Windows XP SP2 and later (or Windows 2000 SP4 and later). It offers both detection (passive scanning) and prevention (active scanning). Windows Defender (beta) is free for Windows users (at the time of this writing).

See the following website to download and try Defender:

http://www.microsoft.com/athome/security/spyware/software

After you install Defender, you will see a little gray castle icon running on your taskbar and a corresponding desktop icon. Defender automatically starts every time Windows starts up and stays running in the background. The main Defender control window looks like Figure 5-12.

A green status means no threats have been detected. You can adjust some of the settings by clicking **Tools > General Settings**, as shown in Figure 5-13.

Some of the recommended settings you want to checkmark are these:

- **Automatically scan my computer** (and you specify the frequency, daily or weekly are recommended, and time of day)
- **Check for updated definitions before scanning**
- **Apply actions on detected items after scanning**

Figure 5-12 Windows Defender Main Status Window

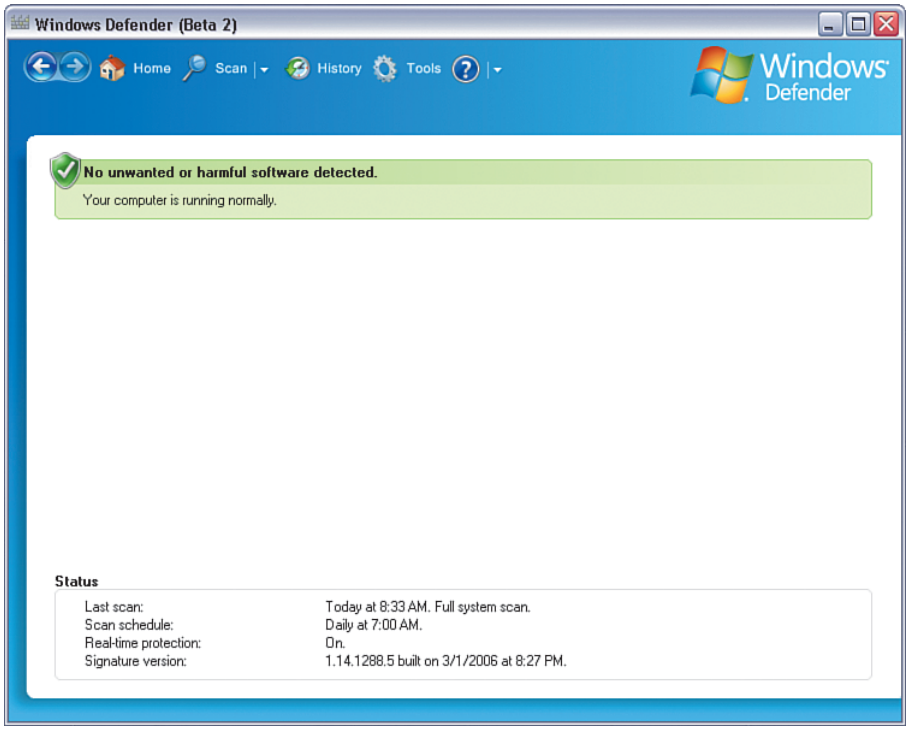
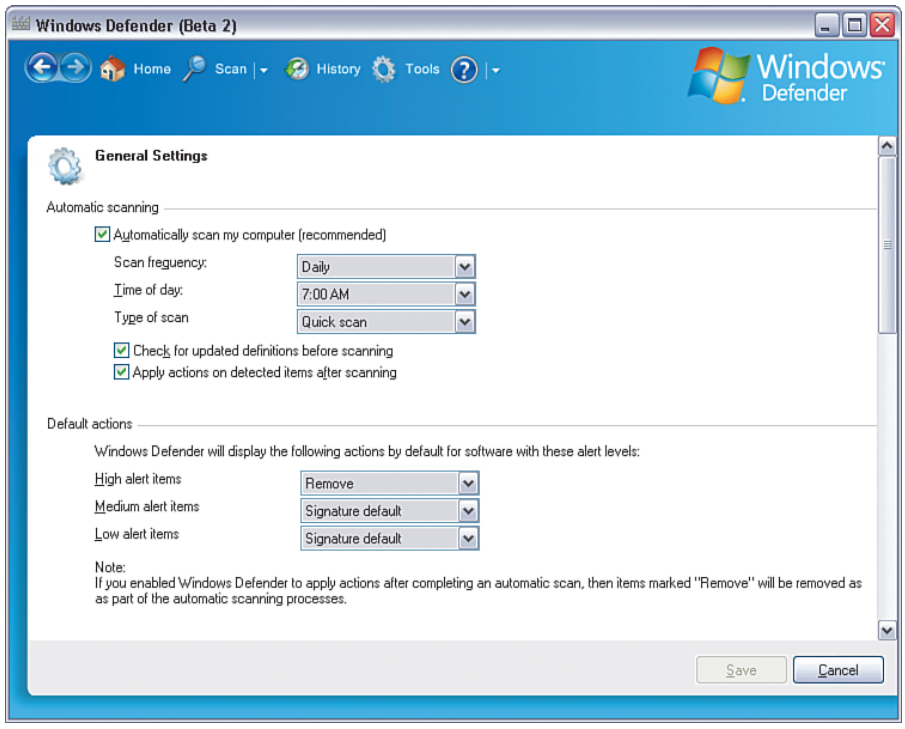
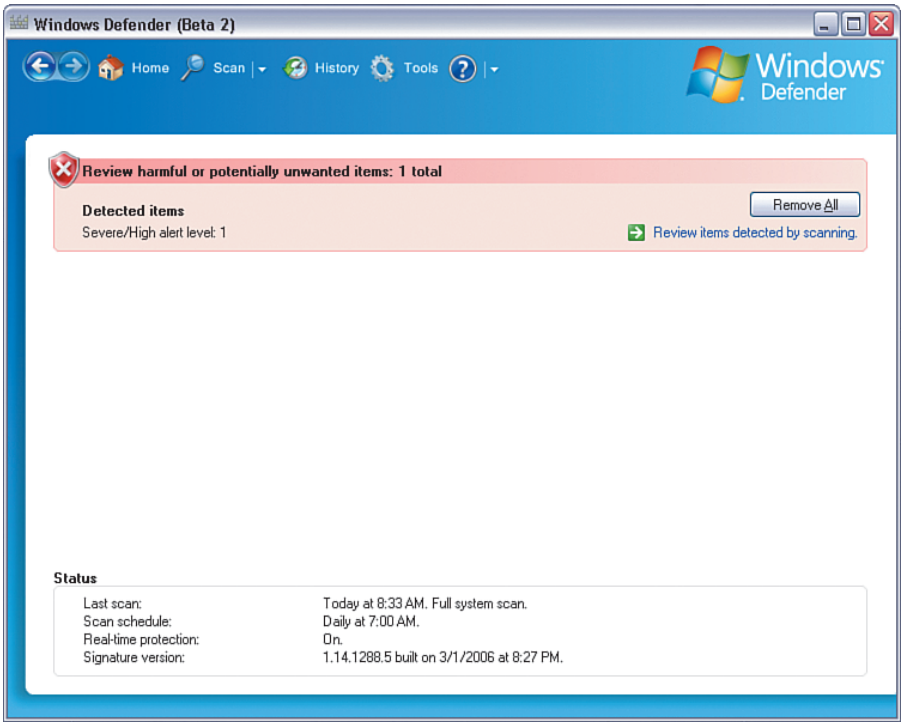


Figure 5-13 Windows Defender Settings



With these settings enabled, Defender will always automatically get the latest adware and spyware signatures over the Internet, and scan your computer periodically. If a problem is found, you will see a red status appear, as shown in Figure 5-14.

Figure 5-14 Windows Defender Detects a Problem



Clicking the warning area takes you to a page where you can manually determine what you want to do with the spyware or adware detected, as shown in Figure 5-15.

The Action options are **Ignore**, **Remove**, or **Allow**. Unless you need it, select **Remove** and then **Apply Actions**. Alternatively, click **Remove All** if you want to get rid of all of it.

Figure 5-16 shows a list of adware that has been removed by Defender.

Figure 5-15 Windows Defender Requests What to Do with Detected Spyware

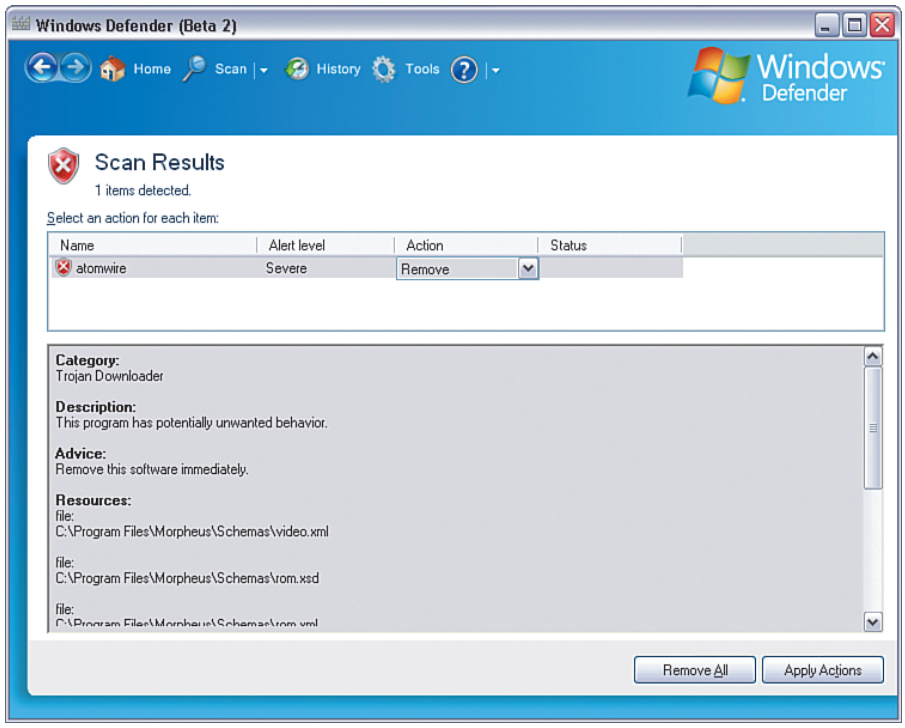
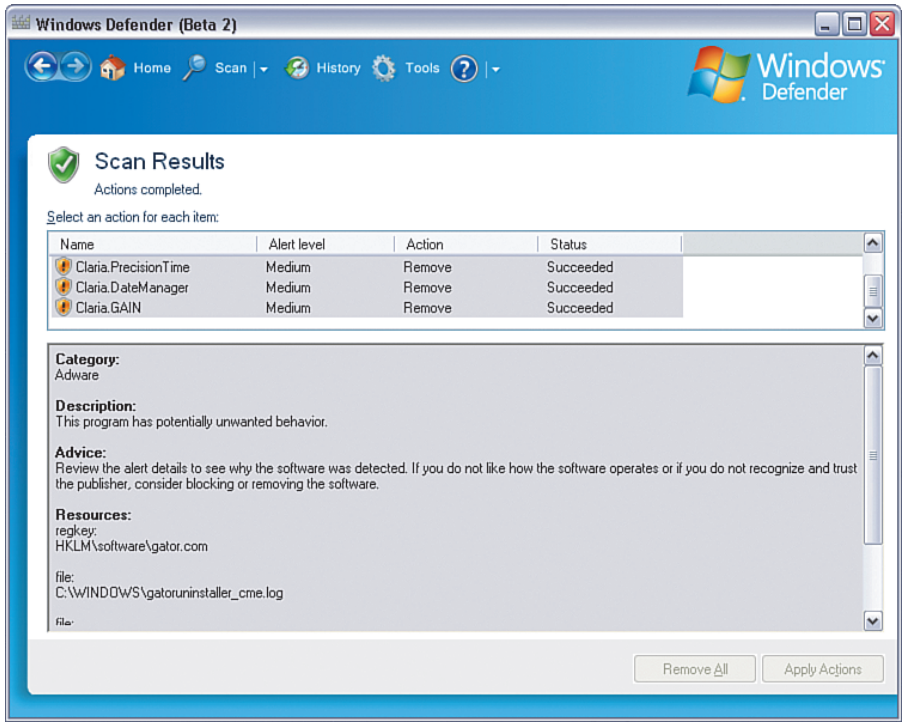


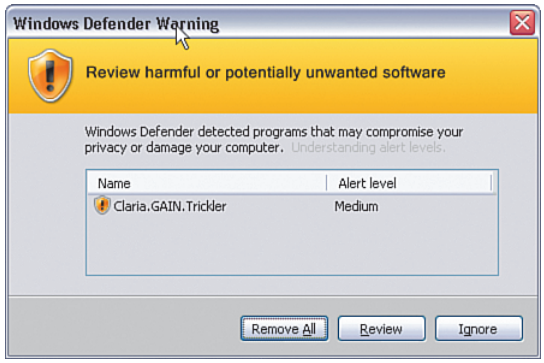
Figure 5-16 Windows Defender Removed Adware



That covers the passive scanning mode of Defender (meaning detecting, and removing spyware/adware when it is already there). Let's now look at Defender's active scanning to see how it can help prevent spyware/adware from being installed in the first place.

Windows Defender runs in the background on your computer. If you click something to install that has spyware or adware associated with it, Defender pops up a warning, such as the example shown in Figure 5-17.

Figure 5-17 Windows Defender Adware/Spyware Warning



You can then avoid installing the software and thereby prevent the adware from getting on your computer. Another cool feature of Defender is the ability to report potential spyware threats back to Microsoft for investigation (so that future versions of Defender can be improved with the latest signatures).

Windows Defender (still in beta, do not forget, but could be production-ready by the time you read this book) seems like a pretty good addition to Windows for security. Adding to that Windows Firewall and Windows Live OneCare antivirus, and it would seem that Microsoft is finally on their way to incorporating much needed security into Windows.

Antispyware/Antiadware in the Security Bundles

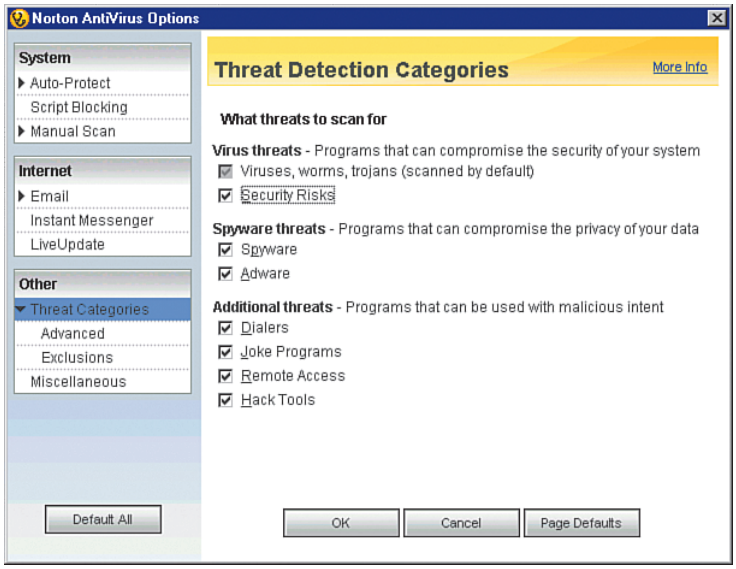
A final option available for antispyware/antiadware is that if you decided to buy or already own one of the security software bundles (such as McAfee Internet Security Suite 200x, Symantec Norton Internet Security 200x, Trend Micro PC-cillin Internet Security, or ZoneAlarm Internet Security Suite), all have an antispyware/antiadware component.

See Table 1-1 (Chapter 1) or Table 3-1 (Chapter 3) for the location of the websites to purchase one of the security bundle products.

For these products, consult the User Guide for how to enable the spyware/adware protection.

Figure 5-18 shows one example for enabling antispyware/antiadware in Symantec's product.

Figure 5-18 Turning On Spyware/Adware Blocking with Symantec Norton Internet Security 200x



What to Do If You Think You've Been Infected

If you think your computer might already be infected with spyware or adware, you are probably correct. If you have never performed a spyware/adware scan before, chances are pretty good you have some.

Some symptoms of spyware/adware can include the following:

- New toolbars or searchbars appearing in your Internet browser
- New programs that you do not recognize appearing in your add/remove programs list
- Sluggish computer performance
- Popup ads that keep appearing

One way to see what is happening in your computer is to check out the running tasks list. In Windows XP, you can press the **Ctrl-Alt-Del** keys simultaneously and then click **Task Manager**. First check the **Performance** tab, which shows you what percentage of your computer's processor is being used over time. If it is excessively high, you could have spyware/adware consuming cycles.

If you do think you have spyware and adware on your computer, you can take a number of steps to remove them.

Spyware/Adware-Removal Tools

The first option is the antispyware/antiadware programs discussed earlier in this chapter. All the options presented scan your computer and detect known adware and spyware programs (and remove them).

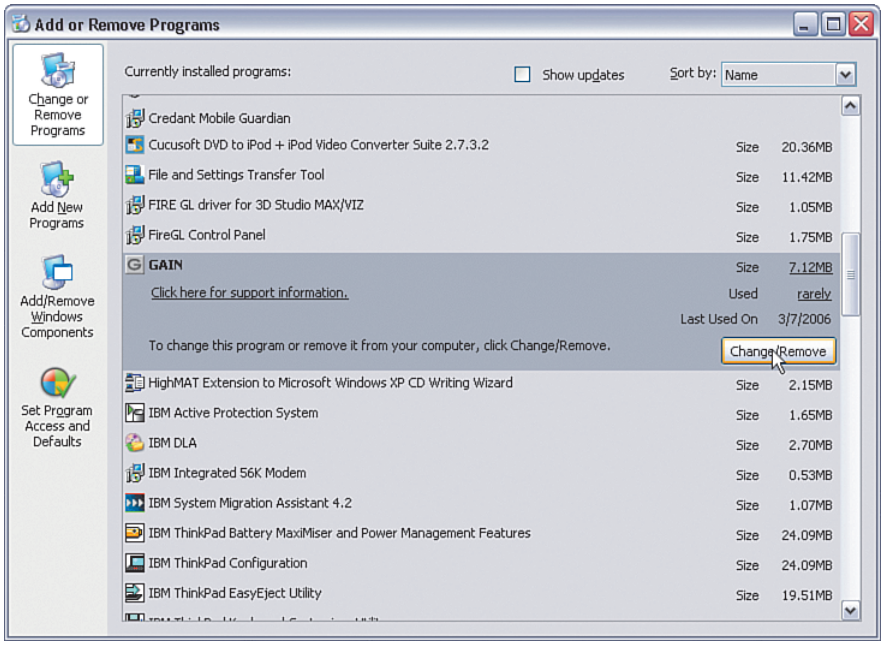
Some adware and spyware will not be completely removable by these tools and might be more stubborn to eradicate.

Removing Spyware and Adware Programs Using the Installed Programs List

If you run across stubborn adware or spyware that cannot be completely removed by the antispyware/antiadware program you are using, you might have to remove the program using the Windows Add/Remove Programs panel.

To do so, click **Start > Control Panel > Add/Remove Programs**. As shown in Figure 5-19, click the program you want to remove, and then click **Change/Remove**.

Figure 5-19 Uninstalling an Unwanted Program



The adware program will be uninstalled. Often, as part of the uninstall process, the adware or spyware will open the Internet browser, go to their website, and ask you to confirm you want to delete it. They will also typically pester you a bit with questions about why you are uninstalling.

In general, it is good practice to become familiar with the programs in the Add/Remove Programs list (and the Program Control list in your personal software firewall). That way, when a new entry unexpectedly appears, you can recognize it.

If you are not sure whether the program is adware/spyware or a legitimate program, the best thing to do is look in the directory under C: /Program Files and get the name of the .exe or .dll file. Then search on the name at one of these online resources:

http://www.pcpitstop.com/spycheck/known.asp

http://www.processlibrary.com

They will tell you whether the program files are spyware/adware or legitimate.

Some adware, spyware, and viruses will not be detected by antispyware/antiadware/antivirus software and will not show up in the Add/Remove Programs list or in your program files. These will be more difficult to remove, and the multitude of possibilities here requires detail no book has room for. If you suspect you have spyware, adware, or a virus and the steps covered previously do not get rid of the symptoms or the problem, you will have to do a bit of research. Go to a trusted security discussion forum and post details about the symptoms or problems you are having. Chances are someone out there has discovered a way to fix the same problem you are having and will share some steps to help you. Remember, only follow steps from a trusted site, such as the support forum at your security product's website.

Summary

Popup blockers are a good first step toward protecting against spyware/adware programs finding their way onto your computer.

Antispyware/antiadware programs offer protection against most spyware and adware threats. Some programs provide passive scanning (detection after infection), whereas others provide both passive and active scanning (detection before infection).

Much like antivirus technology, antispyware/antiadware programs rely on regular updates of signatures to be effective.

Where to Go for More Information

You can learn more about spyware/adware from the following websites:

http://www.microsoft.com/athome/security/spyware

http://www.lavasoft.com/trackware_info

http://www.safer-networking.org/en/tutorial