CISCO SYSTEMS

Home Network Security Simplified

A straightforward, graphic-based reference for securing your home network

ciscopress.com

Jim Doherty
Neil Anderson

Home Network Security Simplified

Jim Doherty
Neil Anderson

Illustrations by Nathan Clement

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

Home Network Security Simplified

Jim Doherty

Neil Anderson

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing July 2006

ISBN: 1-58720-163-1

Library of Congress Cataloging-in-Publication Data

Doherty, Jim, CCNA.
Home network security simplified / Jim Doherty and Neil Anderson.
p. cm.
Includes index.
ISBN 1-58720-163-1 (pbk.)
1. Home computer networks--Security measures. I. Anderson, Neil, 1965- II. Title.
TK5105.75.D638 2007
005.8--dc22
2006019633

Warning and Disclaimer

This book is designed to provide information about home network security. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Publisher
Paul Boger

Cisco Representative
Anthony Wolfenden

Cisco Press Program Manager
Jeff Brady

Senior Editor
Elizabeth Peterson

Managing Editor
Patrick Kanouse

Development Editor
Andrew Cupp

Senior Project Editor
San Dee Phillips

Project Editor
Betsy Harris

Copy Editor
Keith Cline

Technical Editors
Doug Foster
Bradley Mitchell

Editorial Assistant
Vanessa Evans

Cover Designer
Louisa Adair

Book Designer and Compositor
Mark Shirar

Indexer
Tim Wright

Proofreader
Katherin Bidwell

About the Authors

Jim Doherty is the director of marketing and programs with Symbol Technologies' industry solutions group. Prior to joining Symbol, Jim worked at Cisco Systems, where he led various marketing campaigns for IP telephony and routing and switching solutions. Jim has 17 years of engineering and marketing experience across a broad range of networking and communications technologies. Jim is the co-author of the *Networking Simplified* series of books, including *Cisco Networking Simplified*, *Home Networking Simplified*, and *Internet Phone Services Simplified*. He is also the author of the "Study Notes" section of *CCNA Flash Cards and Exam Practice Pack* (CCNA Self-Study, Exam #640-801), Second Edition. Jim is a former Marine Corps sergeant; he holds a bachelor of science degree in electrical engineering from North Carolina State University and an MBA from Duke University.

Neil Anderson is the senior manager of enterprise systems engineering with Cisco Systems. Neil has more than 20 years of broad engineering experience, including public telephone systems, mobile phone systems, Internet, and home networking. At Cisco, Neil's focus is on large corporate customers in the areas of routing and switching, wireless, security, and IP communications. Neil is the co-author of the *Networking Simplified* series of books including, *Home Networking Simplified* and *Internet Phone Services Simplified*. Neil holds a bachelor of science degree in computer science.

About the Illustrator

Nathan Clement declared himself an illustrator a little more than three years ago. Nathan holds a bachelor of fine arts degree in art and writing, which launched a surprise career in publishing, design, and art direction. His major roles have been owning a printing company, designing books in-house at Macmillan Computer Publishing, and serving as art director for an ad agency. Through these little adventures, he decided to get back to his art roots and keep both feet planted in the publishing world as an illustrator. He has been pleased to illustrate three previous books in the Cisco Press *Networking Simplified* series and has done work for Que Publishing, Macromedia Press, Peachpit Press, Prentice Hall, and *ESPN The Magazine*. He lives with his wife, Greta, a nurse practitioner, in Indianapolis and also pursues children's book illustration with paint and brushes. Contact Nathan at nathan@stickman-studio.com.

About the Technical Reviewers

Doug Foster works in the area of packet voice, video, and data convergence. With 30 years of experience for companies such as Cisco Systems, John Deere, Alcatel, and private business, Doug has some interesting firsthand stories to tell about the evolution of the Internet. He has architected and helped install international networks—such as the migration of John Deere's worldwide SNA business network into a multiprotocol intranet in the mid-1980s. As a result of that work, Doug was asked by the U.S. Department of Defense to speak at Interop '88 on "How John Deere builds tractors using TCP/IP." This was nearly a decade before most businesses began to leverage the value of the Internet and eCommerce applications. Most recently, Doug worked for Cisco Systems as one of its first enterprise voice consultants.

Doug has a bachelor of science in mechanical engineering from Iowa State University and lives in Cary, North Carolina, with his wife, Cindy. When not busy with family—daughters, Erin and Amber; son-in-law, Jeremy; and grandson, Jake—or business (Convinsys, Performance Podcasts, and Idea Mechanics), Doug devotes his free time to writing his first book (*Convince Me!*) and to sea kayaking.

Bradley Mitchell works as a freelance writer on the About.com wireless/networking site. He has produced online content at About.com on home computer networking, wireless, and related topics for six years. Bradley is also a senior engineer at Intel Corporation. Over the past 12 years at Intel, he has served in various capacities for research and development of software and network systems. Bradley obtained his master's degree in computer science from the University of Illinois and his bachelor's degree from M.I.T.

Dedications

I would like to dedicate this book to my parents, Jim Doherty and Pierrette Phillips. Dad, thanks for teaching me to be a good kid. Mom, thanks for sticking up for me when I wasn't.

—Jim

I would like to dedicate this book to my parents. I am not exactly sure how, but my dad continues to live in the twenty-first century without touching a computer. That's one way to avoid online identity theft. And to my mom, who despite being the target of several computer viruses, still sees the value in home and business networking.

—Neil

Acknowledgments

Jim and Neil would like to thank the following people:

Our families, for putting up with all the late nights and weekends, rooms full of computers and cables, and for changes we made to their PCs when they were asleep or at school.

Our publisher and the fine team at Cisco Press and Pearson Education. We would especially like to thank our editor, Drew Cupp, who we beat like a rented mule. He not only survived, he also managed to make sense out of our garbled English.

Our illustrator, Nathan Clement at Stickman Studios (www.stickman-studio.com/), who makes all this stuff come to life with great illustrations.

Our technical reviewers, Bradley Mitchell and Doug Foster, who both make sure we do our homework and who keep us from making fools of ourselves by catching our mistakes before you ever see them.

And last but not least, the following people who helped us with technical questions along the way: Stuart Hamilton, Steve Ochmanski, Brian Cox, Lou Ronnau, Max Ardica, and Jason Frazier.

Contents at a Glance

Contents

Introduction

This book provides what we hope is a simplified approach to home network security. Our aim is not to make you a security expert or a network expert or an expert on any other topic. We would, however, like to arm you with some amount of knowledge and know-how so that you can adequately protect your assets (monetary and computer) and identity, which are both at risk when you connect your computer to the Internet. Some level of risk is always present while on the Internet, but the danger can be mitigated. Without knowing what the threats are and how to protect yourself against them, you put yourself in an unnecessarily risky position. Most books on security try to hook you with fear: fear of hackers, fear of viruses, fear of some digital terrorist stealing your credit card numbers and buying an island in the Caribbean. Our approach is different. The best tool for fighting fear is knowledge; knowledge of the real threats (not the hype), knowledge of the types of security available, and probably most important, knowledge of what to do to keep yourself reasonably safe from threats.

We provide this knowledge in the form of actionable steps that you can take to protect yourself. Ten things that, if done correctly, will keep you safe against the most common threats, attacks, hacks, and scams. Will following these 10 steps make your home network 100 percent bulletproof? Not a chance. The only true way to be 100 percent bulletproof is to turn off your computer and bury it in the backyard. But if you do follow these 10 steps, it will give you a reasonable level of security, keeping you about as safe as one can be without becoming a full-fledged security expert and spending a bunch of money.

Why Do I Even Need Network Security in the First Place?

We promised not to jump on the fear-mongering bandwagon, but we do need to help you 1) recognize that threats do exist and 2) understand the nature of the threats so that you can adequately protect yourselves against them. First things first: the threats.

Unless you have been living in a cave for some time (and even then, maybe), you have surely heard about the threat of computer viruses, worms, hackers, scams, and identity thefts. Internet security is big news, and also big business. On a corporate level, companies must protect themselves against intrusion attempts aimed at gaining secret information, and against attempts to shut down corporate websites that provide both the face of a company and a revenue conduit. On the home network side, individuals must protect their personal information, protect their computers from corruption or from being taken over, and protect against others accessing their networks to download illegal or illicit material (or just annoying the heck out of you with endless spam).

If you do connect to the Internet, sooner or later you will see every threat and hack attempt there is. Well, you'll see it if you take no precautions. If you follow the steps we lay out, you will either stop them in the act by recognizing the threat and acting accordingly or prevent them from happening at all and not even be bothered by it.

Threat Categories

One of the things that we have noticed in most of the books and articles on home network security is a lack of any explanation of the different types of security threats. This is a pretty serious issue because many nonexperts lump every type of threat into something called "security," which often leads people into thinking that one type of security solution, say a firewall, will protect them from all the bad stuff out there. This is a big mistake. There are several different types of security threats and one or two things that you can and should do for each type of threat. To help you sort it out, we have grouped threats into four basic categories: connection-based threats, access-based threats, software-based threats, and victim-enabled threats. Each threat category is described here.

Connection-Based Threats

A connection-based threat is an attack that is directed through your Internet connection. This threat exists because high-speed Internet is always on (unlike dialup, which you set up, use, and then break the connection when finished). Hackers typically look for open IP addresses (which represent your location on the Internet) using tools that randomly look for an open connection into an unprotected home network. When hackers find an open network, they can do a number of bad things, including but not limited to, searching through and possibly deleting personal information and files; or using your computer to launch attacks against other home, commercial, or government networks. This latter form of activity is called a redirect attack, a tactic hackers use to protect their own identity and location.

Access-Based Threats

An access-based threat usually results from using a wireless networking device in your home. Just about every wireless router on the market today is made to work right out of the box. This is great for getting your wireless networking up and running quickly, but the only way to make it that easy for you is to turn off all the security features, which makes is easy for everyone else in range of the router to gain access to your network, too. The usual result of not guarding against this threat is that you end up providing all the people around you with free Internet access. This may or may not be an issue for you, but you are also vulnerable to some hackers who can access your files or monitor your network traffic looking for passwords and personal information such as credit card numbers. There is also the risk that someone might be looking to download illicit, indecent, or illegal (sometime all three simultaneously) material from the Internet through your network rather than their own, just in case the feds or someone else come looking for them.

Software-Based Threats

This is probably the threat most people are familiar with. The category includes viruses, worms, spam, spyware, adware, and Trojan horses. Most of the time, these types of attacks are more of an inconvenience than anything else, but the annoyance factor gets pretty high when you get 100 or so unsolicited e-mails every day or if a virus copies your entire contacts list and starts sending copies of itself to everyone you know. Some viruses, though, can damage your computer or files, or worse, deposit a Trojan horse that enables a hacker to take remote control of your computer. All should be guarded against.

Victim-Enabled Threats

The Internet is a scam artist's paradise. Along with the usual array of rip-off scams, the Internet allows thieves to wrap themselves in legitimate-looking letters, web pages, and other wrappers that make it hard for the casual observer to tell the difference between legitimate and illegitimate sites and sources. The good news is that it takes a victim's participation to enable these threats. Unlike the other threats that require hardware or software, this type of threat can usually be solved with a simple set of rules for answering account questions and some education on how to avoid biting on the bait. In addition to identity theft, there is also good old-fashioned theft (someone taking your laptop), so we also provide you with some tips on how to keep folks from cracking your passwords.

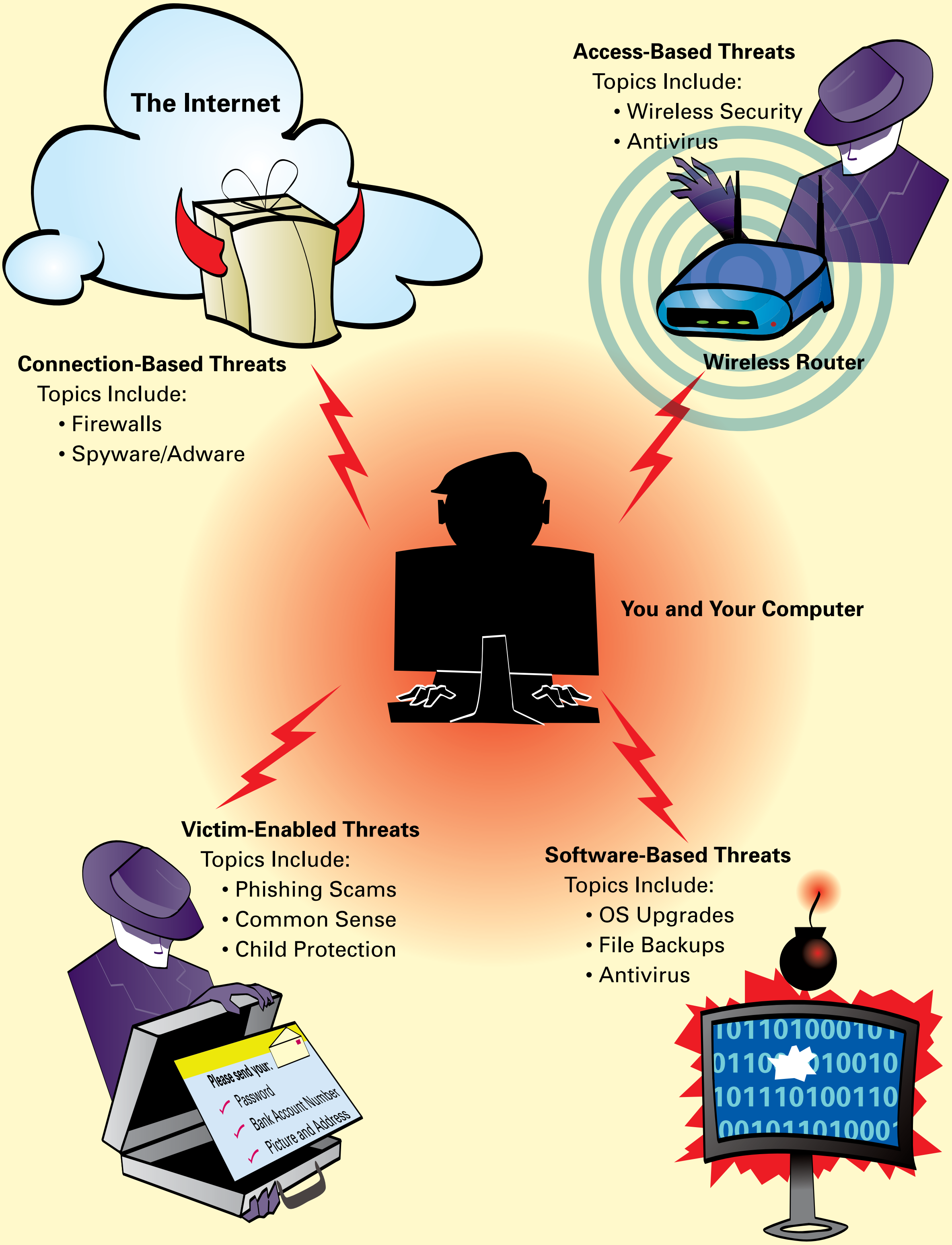
Some of the threats we discuss actually fall into more than one category, and we point those out to you as we go. In addition, we have put a little summary box at the beginning of each chapter that describes the threat, what the issues are, and what you can do about it.

What's to Come?

The rest of this book is set up such that each chapter provides a security tip that you should follow. In each chapter, we describe the category of threat protection and give an example or two of common threats. Nothing too deep, as you really do not need to know, for example, how a virus works in a detailed way; you just need to know how to recognize the threat and, most important, how to protect yourself against it. We also provide a detailed explanation about how to use the hardware, install the software, what to be suspicious of, and when to unplug everything and maybe just go outside and play with the kids.

We recommend that you follow all 10 tips because they all guard against different threats within the 4 threat categories.

To get you started, here is an illustration that describes each threat and shows you the relevant topics. After that, we get right to the business of keeping you, your stuff, and your bank account safe from the bad guys.



Access-Based Threats

Topics Include:

- Wireless Security
- Antivirus

Connection-Based Threats

Topics Include:

- Firewalls
- Spyware/Adware

Victim-Enabled Threats

Topics Include:

- Phishing Scams
- Common Sense
- Child Protection

Software-Based Threats

Topics Include:

- OS Upgrades
- File Backups
- Antivirus

Housekeeping Stuff

This book focuses on the Windows operating systems, and all screen shots were taken from computers running Windows XP Home Edition. If you are not running Windows XP Home Edition, you can still follow the recommendations and tips for the chapters where changes or setups are made or where directory paths are followed. The general steps still hold, but the directory paths and filenames might vary. Your User Manual or help files should help get you where you need to go. In some places, we give special instructions for other operating systems, too.

We also had to make some decisions regarding what type of hardware or programs to install as examples. These are our obvious recommendations, but we also mention good alternatives regarding security equipment or programs. In most cases, turning on the security measures we point out with any equipment fitting the category will be a huge step up from doing nothing at all. When we do make a recommendation, it is usually based on price and performance reasons.

We are not being paid by any of the vendors we refer to in the book, and we do not endorse any particular products. When we do call out and show examples with a specific product, it's because we need to show a tangible example to illustrate how to protect against the security threat being discussed. Feel free to try out the products we show or research and try others.

CHAPTER 5

Tip 5: Lock Out Spyware and Adware

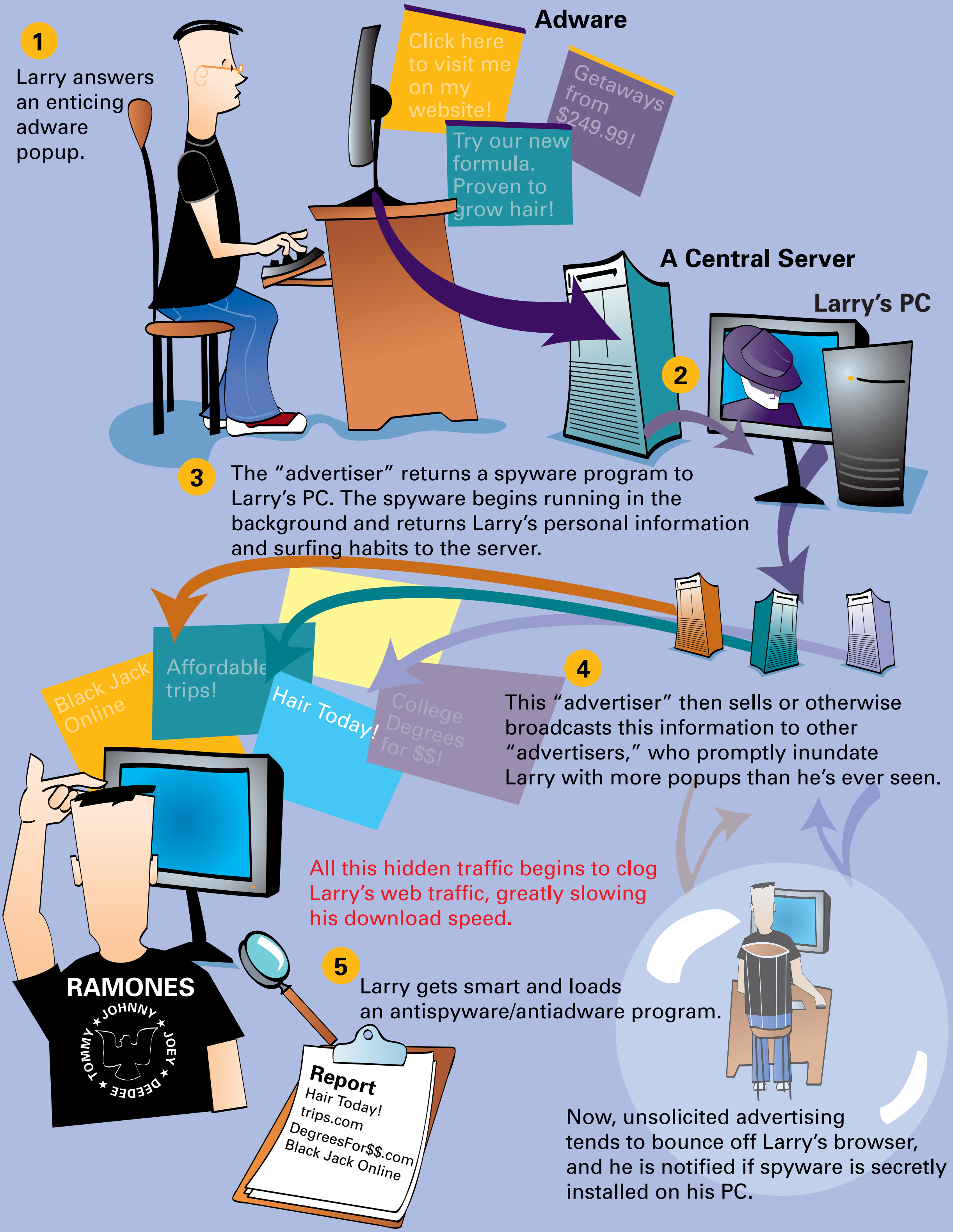
Threat Type: Software based, victim enabled

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.

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.

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.

5 Larry gets smart and loads an antispyware/antiadware program.

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:

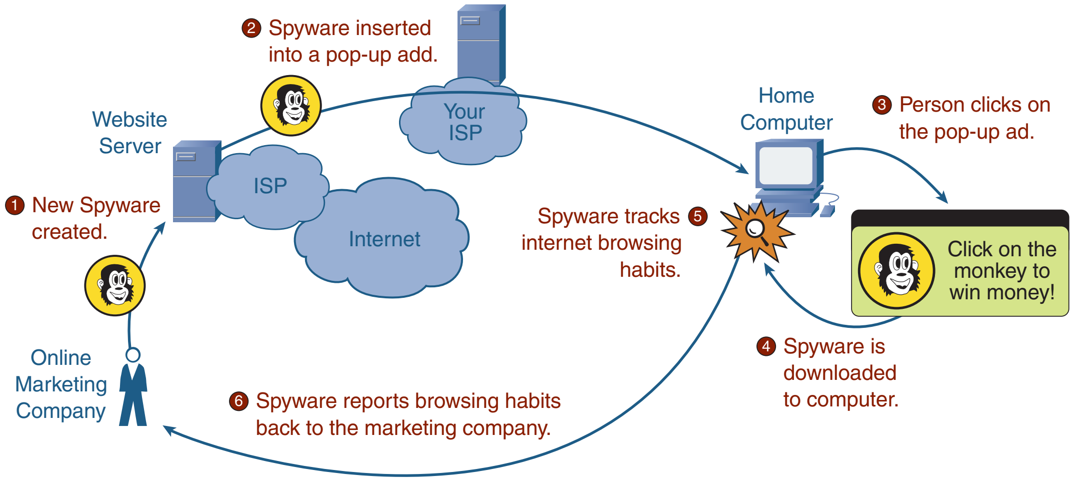
- **Data miners**—Actively collect information from you and then relay it to a remote server.
- **Spyware**—As in the adware case, this term is used for both the category and for a particular instance within the category. In this case, we are referring to a hidden program that collects information and 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


2 Spyware inserted into a pop-up add.
Your ISP
Website Server
ISP
Internet
Home Computer
3 Person clicks on the pop-up ad.
1 New Spyware created.
Spyware tracks 5 internet browsing habits.
Click on the monkey to win money!
4 Spyware is downloaded to computer.
Online Marketing Company
6 Spyware reports browsing habits back to the marketing company.

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.

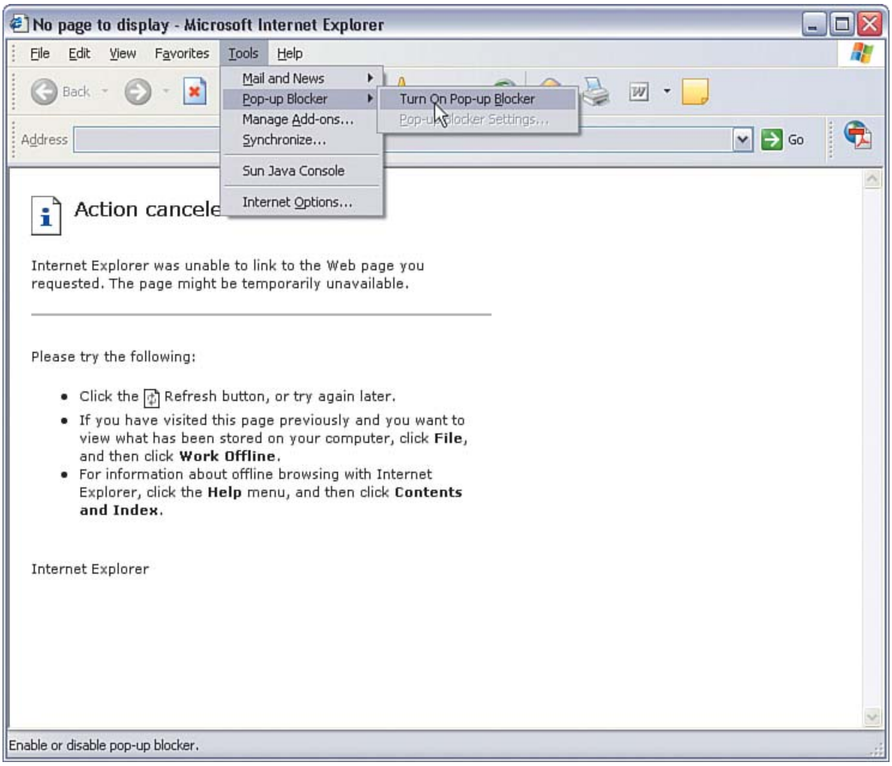
Installing a Third-Party Popup Blocker Program

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



Action canceled

Internet Explorer was unable to link to the Web page you requested. The page might be temporarily unavailable.

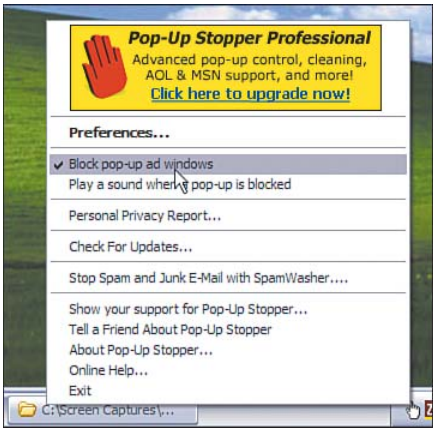
Please try the following:

- Click the Refresh button, or try again later.
- If you have visited this page previously and you want to view what has been stored on your computer, click **File**, and then click **Work Offline**.
- For information about offline browsing with Internet Explorer, click the **Help** menu, and then click **Contents and Index**.

Internet Explorer

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

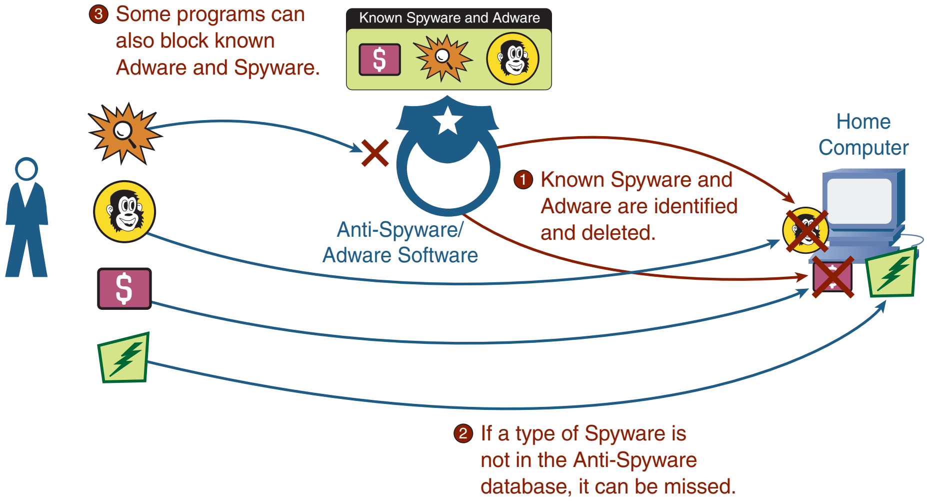

Pop-Up Stopper Professional
Advanced pop-up control, cleaning, AOL & MSN support, and more!
Click here to upgrade now!
Preferences...
✓ Block pop-up ad windows
Play a sound when a pop-up is blocked
Personal Privacy Report...
Check For Updates...
Stop Spam and Junk E-Mail with SpamWasher....
Show your support for Pop-Up Stopper...
Tell a Friend About Pop-Up Stopper
About Pop-Up Stopper...
Online Help...
Exit
C:\Screen Captures\...

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



3 Some programs can also block known Adware and Spyware.
Known Spyware and Adware
$
Home Computer
1 Known Spyware and Adware are identified and deleted.
Anti-Spyware/ Adware Software
$
2 If a type of Spyware is not in the Anti-Spyware database, it can be missed.

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.

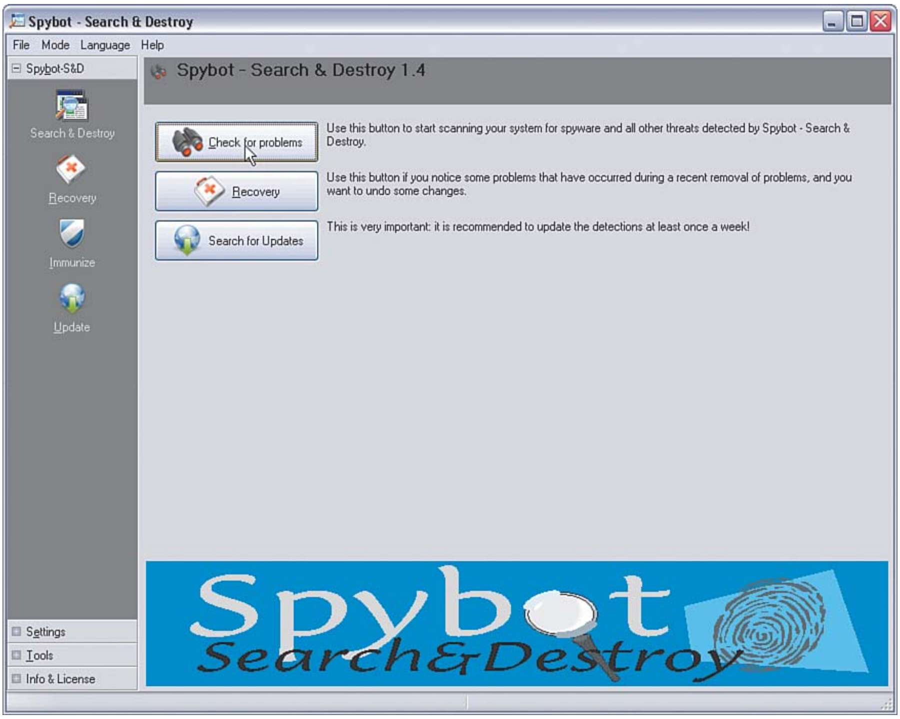
Spybot Search & Destroy

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



Use this button to start scanning your system for spyware and all other threats detected by Spybot - Search & Destroy.

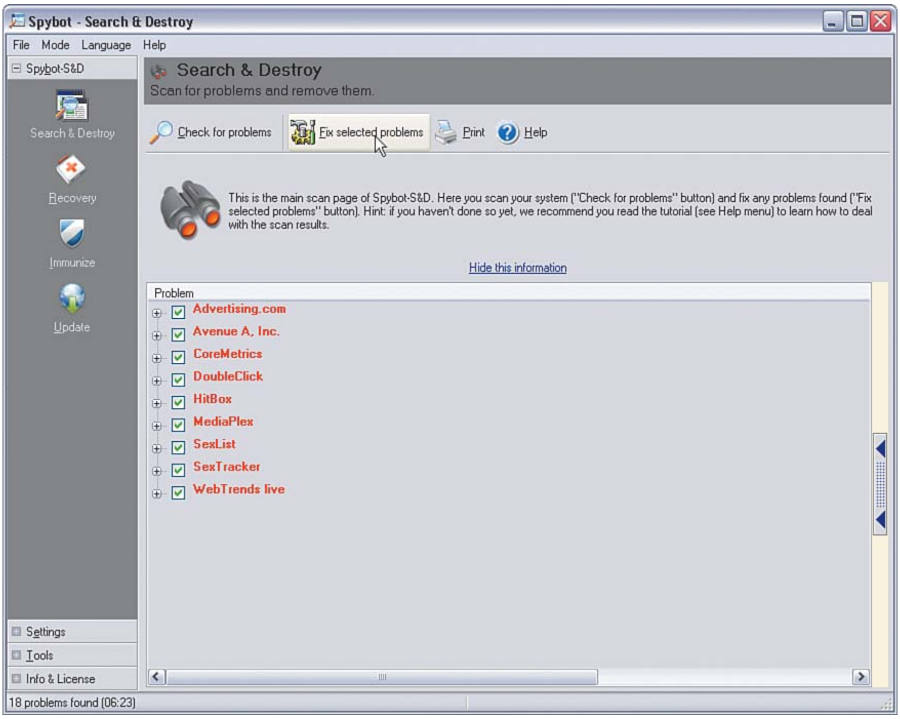
Use this button if you notice some problems that have occurred during a recent removal of problems, and you want to undo some changes.

This is very important: it is recommended to update the detections at least once a week!

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



This is the main scan page of Spybot-S&D. Here you scan your system ("Check for problems" button) and fix any problems found ("Fix selected problems" button). Hint: if you haven't done so yet, we recommend you read the tutorial (see Help menu) to learn how to deal with the scan results.

- ☑ Advertising.com
- ☑ Avenue A, Inc.
- ☑ CoreMetrics
- ☑ DoubleClick
- ☑ HitBox
- ☑ MediaPlex
- ☑ SexList
- ☑ SexTracker
- ☑ WebTrends live

18 problems found (06:23)

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

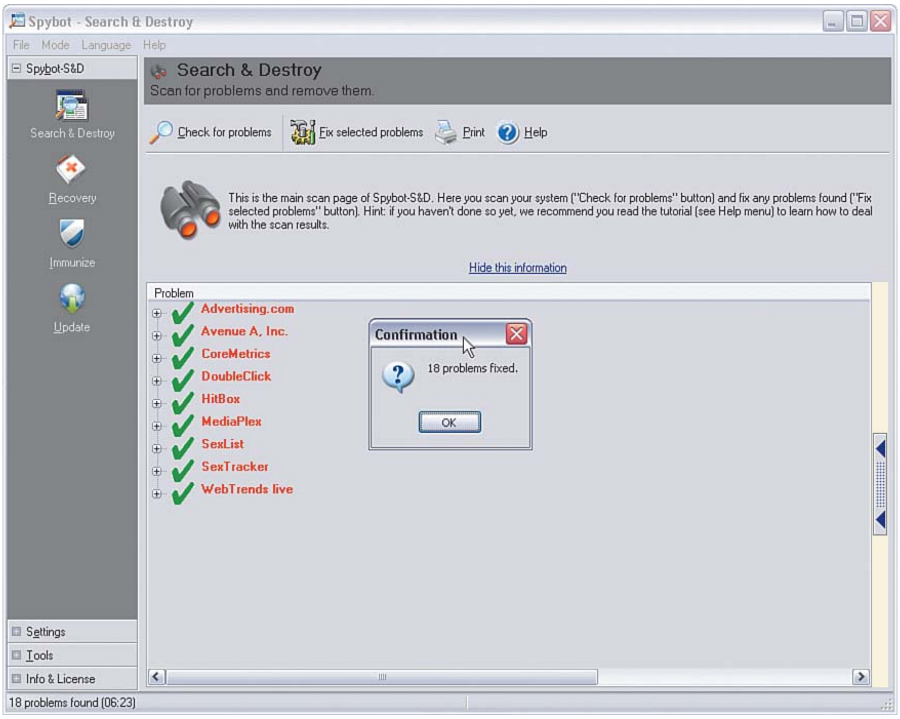
VERY IMPORTANT: Some adware programs are on your computer because you downloaded something, such as a screensaver program, that you are using for free under the agreement that the adware can live on your computer and bring you advertisements. If you remove the adware with Spybot or any other tool, you 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



This is the main scan page of Spybot-S&D. Here you scan your system ("Check for problems" button) and fix any problems found ("Fix selected problems" button). Hint: if you haven't done so yet, we recommend you read the tutorial (see Help menu) to learn how to deal with the scan results.

Problem
- ✓ Advertising.com
- ✓ Avenue A, Inc.
- ✓ CoreMetrics
- ✓ DoubleClick
- ✓ HitBox
- ✓ MediaPlex
- ✓ SexList
- ✓ SexTracker
- ✓ WebTrends live

18 problems fixed.

18 problems found (06:23)

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:

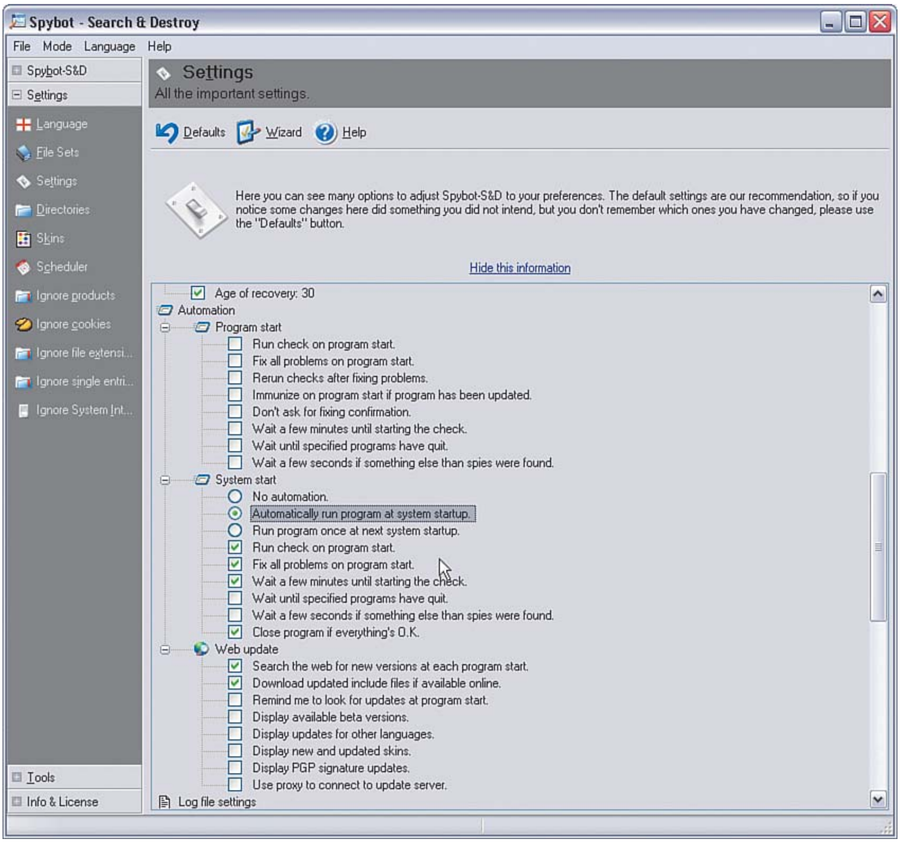
- **Automatically run program at system startup.**
- **Run check on program start.**
- **Fix all problems on program start.**
- **Wait a few minutes until starting the check.**
- **Close program if everything's O.K.**

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



Settings
All the important settings.

Here you can see many options to adjust Spybot-S&D to your preferences. The default settings are our recommendation, so if you notice some changes here did something you did not intend, but you don't remember which ones you have changed, please use the "Defaults" button.

☑ Age of recovery: 30

Automation

Program start

- □ Run check on program start.
- □ Fix all problems on program start.
- □ Rerun checks after fixing problems.
- □ Immunize on program start if program has been updated.
- □ Don't ask for fixing confirmation.
- □ Wait a few minutes until starting the check.
- □ Wait until specified programs have quit.
- □ Wait a few seconds if something else than spies were found.

System start

- ○ No automation.
- ● Automatically run program at system startup.
- ○ Run program once at next system startup.
- ☑ Run check on program start.
- ☑ Fix all problems on program start.
- ☑ Wait a few minutes until starting the check.
- □ Wait until specified programs have quit.
- □ Wait a few seconds if something else than spies were found.
- ☑ Close program if everything's O.K.

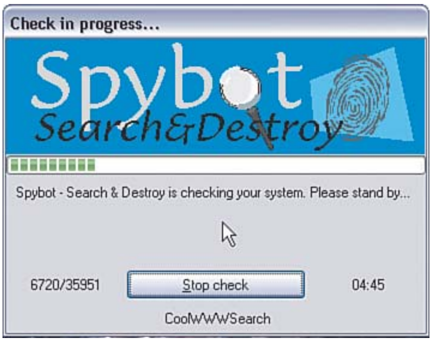
Web update

- ☑ Search the web for new versions at each program start.
- ☑ Download updated include files if available online.
- □ Remind me to look for updates at program start.
- □ Display available beta versions.
- □ Display updates for other languages.
- □ Display new and updated skins.
- □ Display PGP signature updates.
- □ Use proxy to connect to update server.

Log file settings

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



Spybot - Search & Destroy is checking your system. Please stand by...

6720/35951 04:45

CoolWWWSearch

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

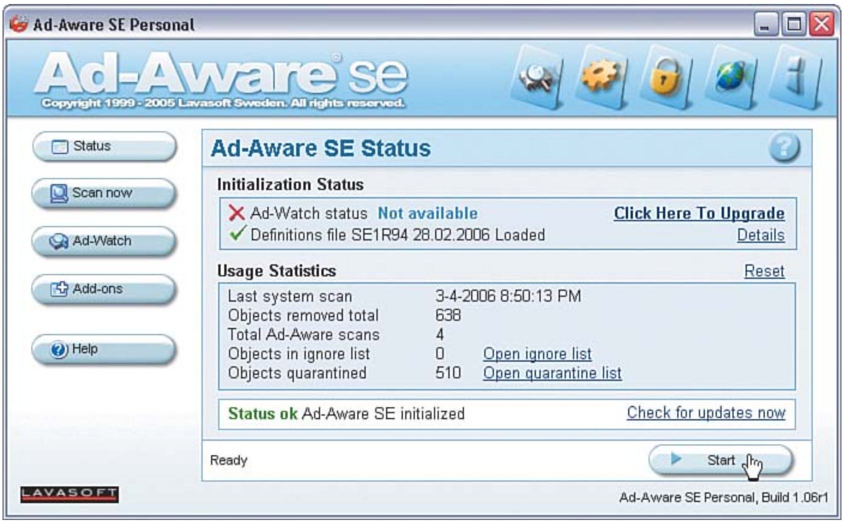
The next product to consider is called Ad-Aware from Lavasoft (a Swedish company; apparently Europeans hate adware and spyware even more than Americans).

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



Ad-Aware SE Status

Initialization Status

✗ Ad-Watch status Not available — Click Here To Upgrade
✓ Definitions file SE1R94 28.02.2006 Loaded — Details

Usage Statistics — Reset

Last system scan	3-4-2006 8:50:13 PM	
Objects removed total	638	
Total Ad-Aware scans	4	
Objects in ignore list	0	Open ignore list
Objects quarantined	510	Open quarantine list

Status ok Ad-Aware SE initialized — Check for updates now

Ready — Start

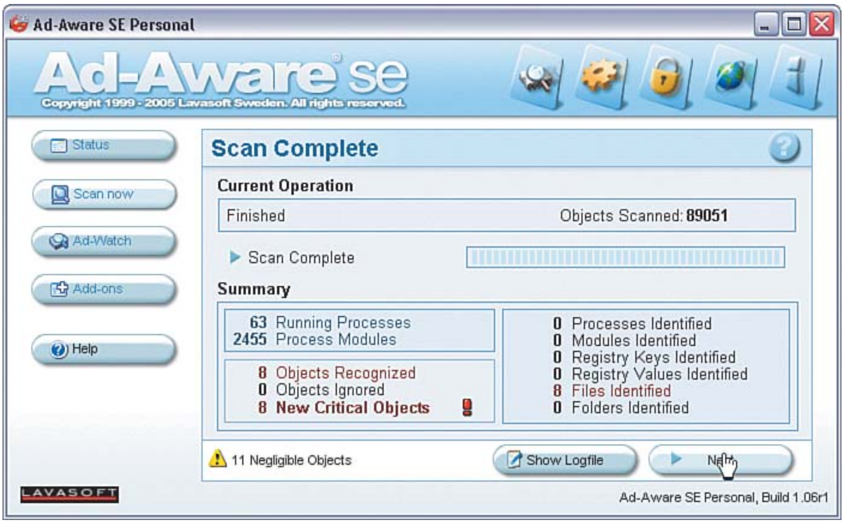
Ad-Aware SE Personal, Build 1.06r1

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



Scan Complete

Current Operation

Finished Objects Scanned: 89051

Scan Complete

Summary

63 Running Processes
2455 Process Modules

8 Objects Recognized
0 Objects Ignored
8 New Critical Objects

0 Processes Identified
0 Modules Identified
0 Registry Keys Identified
0 Registry Values Identified
8 Files Identified
0 Folders Identified

11 Negligible Objects

Ad-Aware SE Personal, Build 1.06r1

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

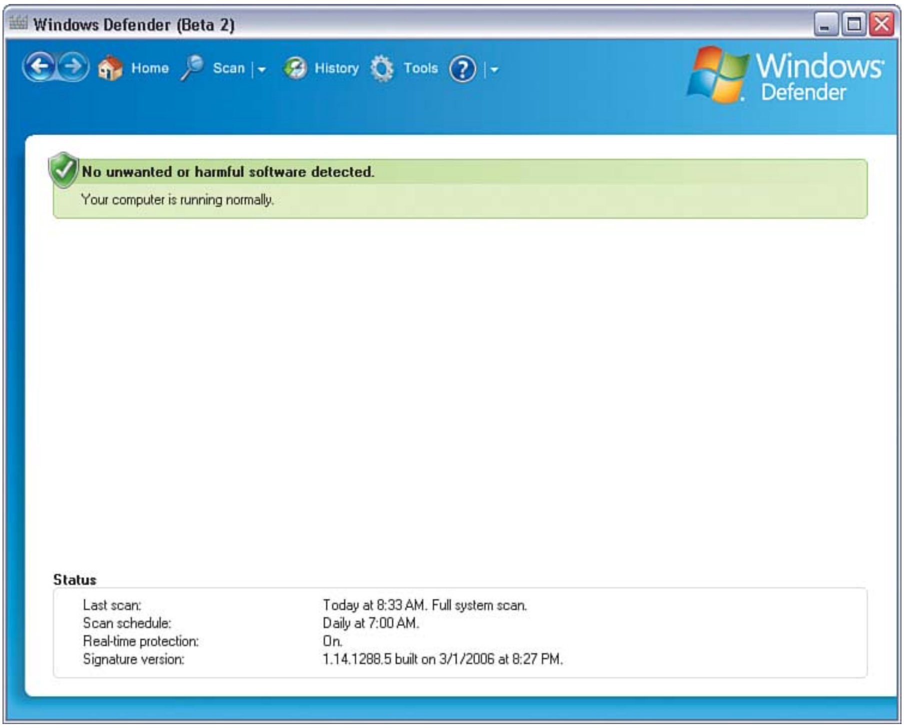
After you install Defender, you will see a little gray castle icon running on your taskbar and a corresponding desktop icon. Defender automatically starts every time Windows starts up and stays running in the background. The main Defender control window looks like Figure 5-12.

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



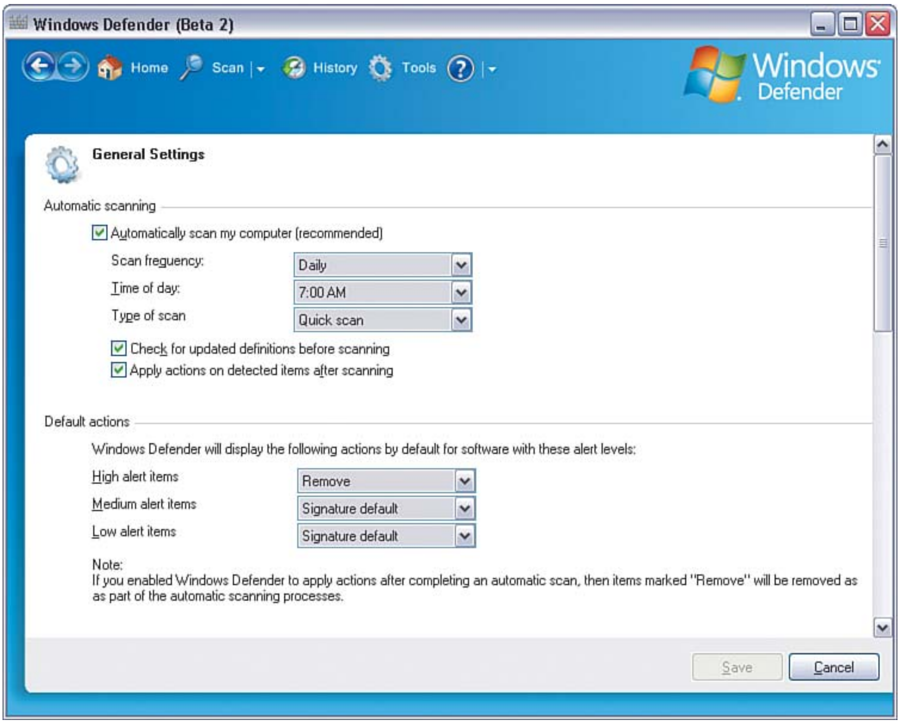
No unwanted or harmful software detected.

Your computer is running normally.

Status

Last scan:	Today at 8:33 AM. Full system scan.
Scan schedule:	Daily at 7:00 AM.
Real-time protection:	On.
Signature version:	1.14.1288.5 built on 3/1/2006 at 8:27 PM.

Figure 5-13 Windows Defender Settings



General Settings

Automatic scanning

☑ Automatically scan my computer (recommended)

Scan frequency:	Daily
Time of day:	7:00 AM
Type of scan	Quick scan

☑ Check for updated definitions before scanning

☑ Apply actions on detected items after scanning

Default actions

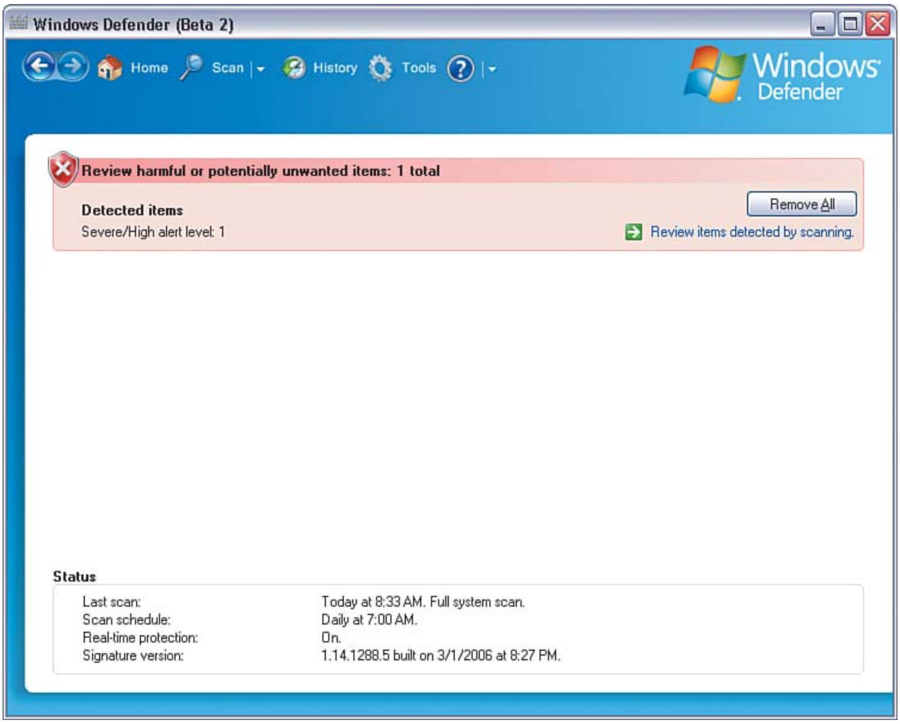
Windows Defender will display the following actions by default for software with these alert levels:

High alert items	Remove
Medium alert items	Signature default
Low alert items	Signature default

Note:
If you enabled Windows Defender to apply actions after completing an automatic scan, then items marked "Remove" will be removed as as part of the automatic scanning processes.

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



Review harmful or potentially unwanted items: 1 total

Detected items
Severe/High alert level: 1

Review items detected by scanning.

Status

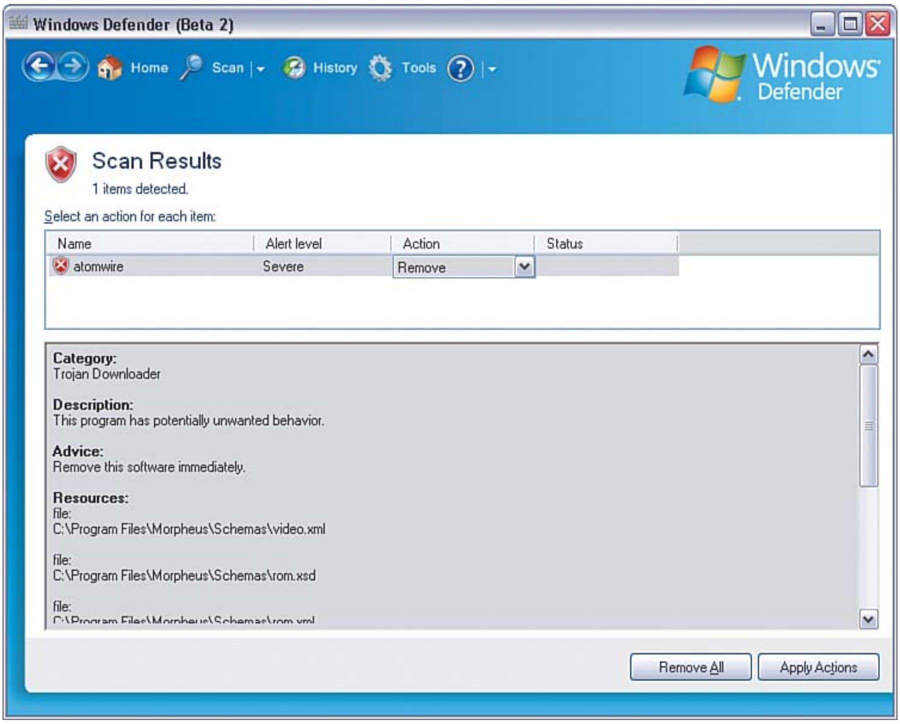
Last scan:	Today at 8:33 AM. Full system scan.
Scan schedule:	Daily at 7:00 AM.
Real-time protection:	On.
Signature version:	1.14.1288.5 built on 3/1/2006 at 8:27 PM.

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



Scan Results

1 items detected.

Select an action for each item:

Name	Alert level	Action	Status
atomwire	Severe	Remove	

Category:
Trojan Downloader

Description:
This program has potentially unwanted behavior.

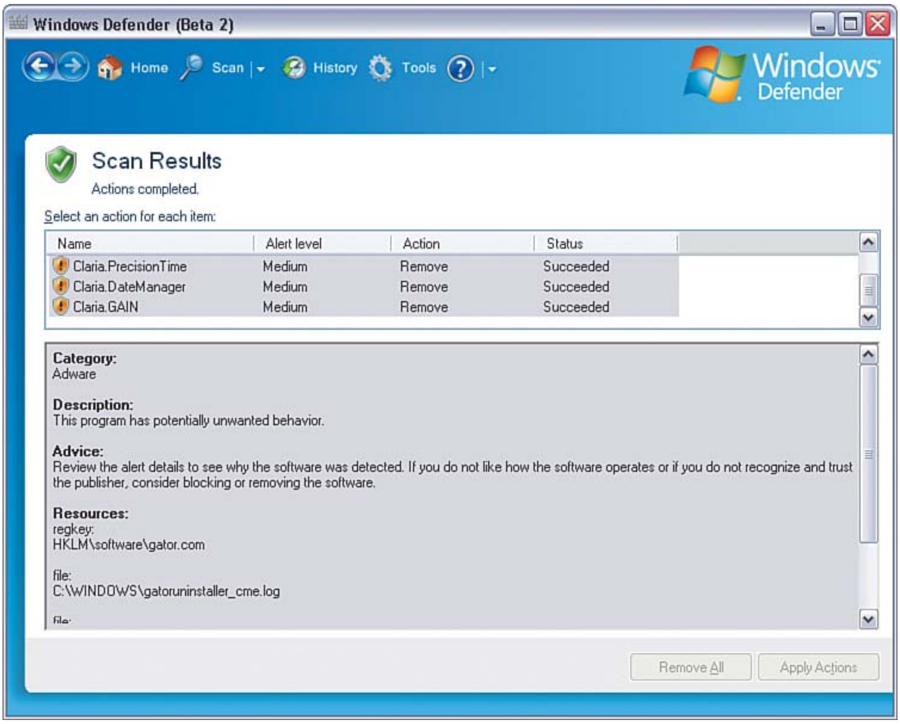
Advice:
Remove this software immediately.

Resources:
file:
C:\Program Files\Morpheus\Schemas\video.xml

file:
C:\Program Files\Morpheus\Schemas\rom.xsd

file:
C:\Program Files\Morpheus\Schemas\rom.xml

Figure 5-16 Windows Defender Removed Adware



Scan Results

Actions completed.

Select an action for each item:

Name	Alert level	Action	Status
Claria.PrecisionTime	Medium	Remove	Succeeded
Claria.DateManager	Medium	Remove	Succeeded
Claria.GAIN	Medium	Remove	Succeeded

Category:
Adware

Description:
This program has potentially unwanted behavior.

Advice:
Review the alert details to see why the software was detected. If you do not like how the software operates or if you do not recognize and trust the publisher, consider blocking or removing the software.

Resources:
regkey:
HKLM\software\gator.com

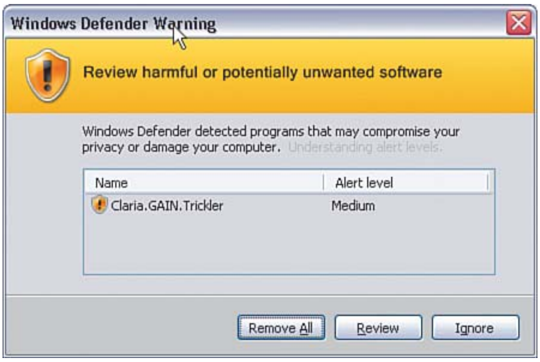
file:
C:\WINDOWS\gatoruninstaller_cme.log

file:

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



Windows Defender Warning

Review harmful or potentially unwanted software

Windows Defender detected programs that may compromise your privacy or damage your computer. Understanding alert levels.

Name	Alert level
Claria.GAIN.Trickler	Medium

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

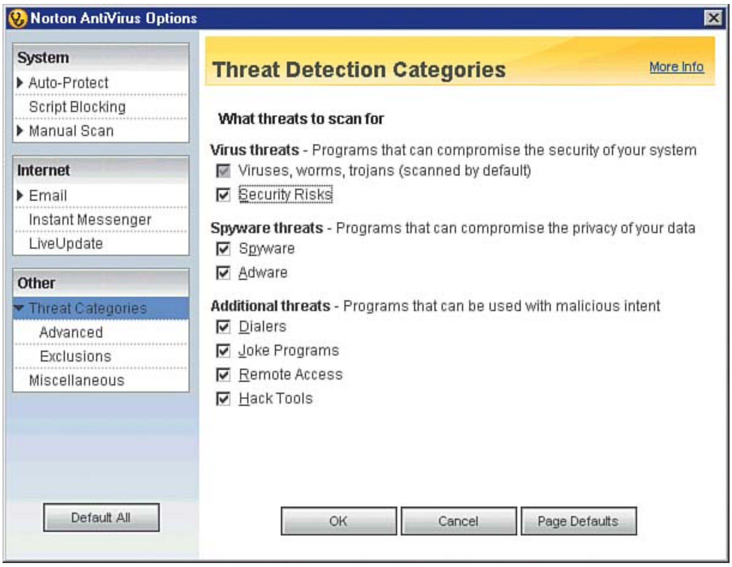
A final option available for antispyware/antiadware is that if you decided to buy or already own one of the security software bundles (such as McAfee Internet Security Suite 200x, Symantec Norton Internet Security 200x, Trend Micro PC-cillin Internet Security, or ZoneAlarm Internet Security Suite), all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



Threat Detection Categories

What threats to scan for

Virus threats - Programs that can compromise the security of your system

☑ Viruses, worms, trojans (scanned by default)

☑ Security Risks

Spyware threats - Programs that can compromise the privacy of your data

☑ Spyware

☑ Adware

Additional threats - Programs that can be used with malicious intent

☑ Dialers

☑ Joke Programs

☑ Remote Access

☑ Hack Tools

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).

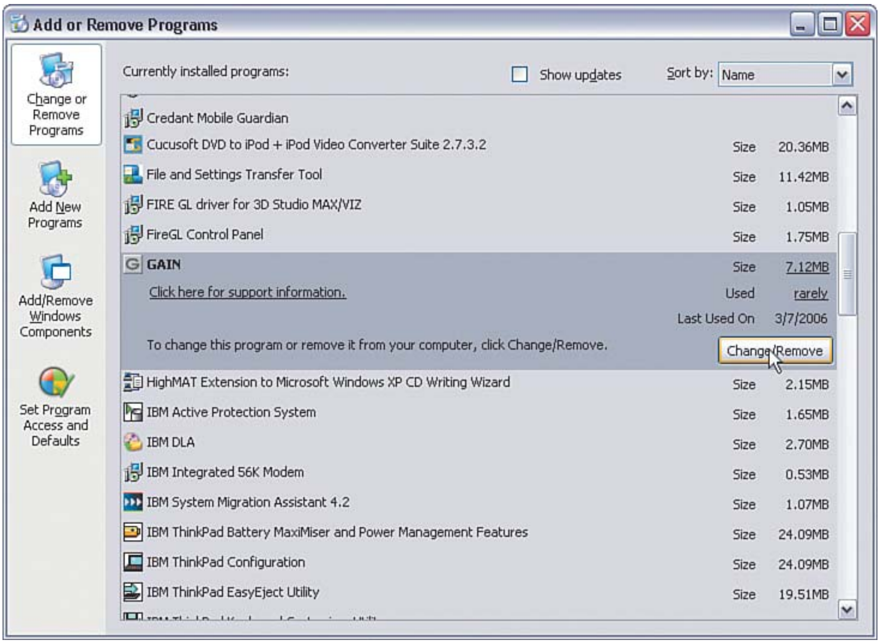
Some adware and spyware will not be completely removable by these tools and might be more stubborn to eradicate.

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


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
☐ Show updates
Sort by: Name
Change/Remove

Currently installed programs:

Credant Mobile Guardian		
Cucusoft DVD to iPod + iPod Video Converter Suite 2.7.3.2	Size	20.36MB
File and Settings Transfer Tool	Size	11.42MB
FIRE GL driver for 3D Studio MAX/VIZ	Size	1.05MB
FireGL Control Panel	Size	1.75MB
GAIN	Size	7.12MB
Click here for support information.	Used	rarely
	Last Used On	3/7/2006
To change this program or remove it from your computer, click Change/Remove.		
HighMAT Extension to Microsoft Windows XP CD Writing Wizard	Size	2.15MB
IBM Active Protection System	Size	1.65MB
IBM DLA	Size	2.70MB
IBM Integrated 56K Modem	Size	0.53MB
IBM System Migration Assistant 4.2	Size	1.07MB
IBM ThinkPad Battery MaxiMiser and Power Management Features	Size	24.09MB
IBM ThinkPad Configuration	Size	24.09MB
IBM ThinkPad EasyEject Utility	Size	19.51MB

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

This page intentionally left blank

INDEX