

Windows **LOCKDOWN!**

**Your XP and Vista Guide Against Hacks,
Attacks, and Other Internet Mayhem**



Windows Lockdown! Your XP and Vista Guide Against Hacks, Attacks, and Other Internet Mayhem

Copyright © 2009 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-3672-7

ISBN-10: 0-7897-3672-1

Library of Congress Cataloging-in-Publication data is on file.

Printed in the United States of America

First Printing: July 2008

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Que Publishing 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.

Windows is a registered trademark of Microsoft Corporation.

Associate Publisher

Greg Wiegand

Acquisitions Editor

Rick Kughen

Development Editor

Rick Kughen

Managing Editor

Patrick Kanouse

Project Editor

Mandie Frank

Copy Editor

Margaret Berson

Indexer

Ken Johnson

Proofreader

Matt Purcell

Technical Editor

Mark Reddin

Publishing Coordinator

Cindy Teeters

Designer

Ann Jones

Composition

Mark Shirar

Introduction: Ignore This Book at Your Own Peril!

As I started to write this introduction, a disturbing statistic arrived in my inbox. Security software maker F-Secure reported that the total number of viruses and Trojans will hit one million by 2009.

One million viruses! That's astounding. Now for the good news: The reason so many are being written is that it's become more difficult for these infections to succeed in infecting systems. That's because security practices have been improved. Computer owners are more educated. Security software is increasingly effective. We are simply more savvy about computer security. And that's great!

In response, the bad guys are shifting their strategies and using new tools to make their malware more effective against us. So while much has changed since I wrote the first edition of this book, much is still the same. The hacks, attacks, and scams keep coming.

So sitting back smugly is not the thing to do now. It's clear to me that we have to always be one step ahead in this game. And that's why I wrote this book.

The first version of this book was first released in 2005 as the *Absolute Beginner's Guide to Security, Spam, Spyware, and Viruses*. Back then it had become clear that malware had shifted from being an ego trip for its authors to a source of revenue. Viruses and spyware and other electronic trickery, like phishing and spam, made money for their authors.

This book builds on the original book, expanding on what has changed since 2005—like the arrival of Windows Vista—and adding lots more useful information.

In this book, I'll show you how to cleanse your computer, halt further infections, sidestep scams, do major damage control, plan for the future, and lock down Windows XP and Vista nice and tight.

To that end, I've updated and added new content to every chapter and written two new ones, including Chapter 3 on rootkits, and Chapter 8 on how to remove infections.

By the time you get through the whole book, you'll not only be able to protect yourself and your family from the threats out there on the Internet, but you'll be well equipped to help your grandma, your friends, your co-workers, and anyone who owns a computer and is not properly protected.

So congratulations on picking up this book, because it shows a commitment to the malware writer that you will not be defeated. There may be one million

malware programs out there, but they'll have to write even more to keep up with us.

I say bring on the next million!

How This Book Is Organized

Chapter 1—Viruses: Attack of the Malicious Programs

In this first and vividly exciting chapter, I tell you what viruses are, why they are a problem, and how to get rid of them. Plus, you will learn secrets, such as the real reason people write viruses in the first place.

Chapter 2—Spyware: Overrun by Advertisers, Hijackers, and Opportunists

Spyware is a modern-day computer pandemic. Your computer is probably rife with this malware. Bad companies are making money with it learning what you do on your computer. At the same time, spyware is also slowing your computer down. Most people experience a 30%–50% performance boost when they get rid of spyware for the first time. How's that for an upsell?

Chapter 3—Rootkits: Sneaky, Stealthy Toolboxes

Root kits were made famous by Sony's blundering move to sneak them onto computers using their music CDs. But the problem is much bigger than that. Learn why rootkits, when used by malware writers, make it difficult to remove infections.

Chapter 4—Hackers: There's a Man in My Machine

Who are the hackers? And why do they want to get into your computer? I tell you why and then show you how to shut them out. And I make a good joke about cheese in this chapter.

Chapter 5—Identity Thieves and Phishers: Protect Your Good Name and Bank Account

These people are going to suck your bank account dry. And they trick you into helping them do it. I show you how to stop them.

Chapter 6—Spam: Unwanted Email from Hell

Junk mail is a deluge, but like a Shop Vac on spilled ketchup, it's easy to clean up. I'll show you how in only a few pages.

Chapter 7—Wireless Network Snoops: Lock Down Your Wi-Fi Network

Let's pretend you're free of all the other nasties in this book, but I bet if you have a wireless home network, your neighbors are using your Internet connection and maybe even snooping in places they shouldn't be inside your computer. I help you stop them.

Chapter 8—Damage Control: How to Remove Viruses and Spyware

This is the chapter you go to after shrieking: "Oh no! I have a virus!" Most people will buy this book for this chapter alone because I show you how to get rid of an infection here.

Chapter 9—Ground Up Security: Wipe Your Hard Drive and Build a Secure Windows PC from the Ground Up

When all else fails, you can always wipe your system clean and start fresh. This chapter shows you how to scrub your system and rebuild it so it really is locked down!

Chapter 10—Ongoing Maintenance: Fend Off Future Threats!

Learn what you need to do to keep your system running infection-free for the rest of your days. Lots of cool strategies that are easy to learn.

Chapter 11—Selecting Software: Steals, Deals, and Software Duds

Next, I'll go over what the story is with lots of different security software. Do you have to buy it or can you get it all free?

Chapter 12—Tools of the Trade: Security Products You Should Own

And in the final chapter I'll tell you what software is really good and where to get it.

Glossary: Computer Threat Lingo

Also, my talented assistant, Ted Gallardo has written the best and most exciting glossary you have ever read. It's really scintillating and has been nominated for glossary of the year.

Special Elements Used in this Book

You'll also see a lot of help in the margins of this book. Here's how it looks and what it means.

note **Notes**—This is stuff that I figured I should tell you when it popped into my head. Notes aren't essential reading, but I urge you not to skip them as you'll learn a lot of extra stuff here that you might not find elsewhere.

tip **Tips**—These succulent bits of info should help you with odd problems or give you insight into issues that are confusing. Don't skip these! Here, you'll find faster ways to accomplish tasks, insider tidbits, and expert tips I've accumulated along the way.

caution **Cautions**—These blurbs keep you out of trouble. I hope. If you don't read these, you're asking for trouble. Security is risky business. I've done my best to point out common pitfalls, gotchas, and other assorted nasties.

SIDEBARS

Occasionally, I've added some additional information that's ancillary to the main topic, but still worth reading. Think of these as important stuff that didn't fit anywhere within the confines of the chapter you're reading, but is too important to skip.

Reader Competition...of Sorts

If you are one of the first 10 people to tell me the name of the guy that wrote the HijackThis program and what page he is mentioned on, I'll send you a copy of my fun and informative DVD, "Getting Started with Windows Vista." Learn more about this blockbuster DVD at www.gettingstartedvideo.com.

When you email me at lockdown@cyberwalker.com, include the answer and your full name, and put "Windows Lockdown Contest" in the subject line.

Finally, if you want to contact me and say nice things, tell me about how you saved your grandma with advice from this book, or send me chocolate cake (which I also love), email me at andy@cyberwalker.com.

Spam: Unwanted Email from Hell

This chapter explains why you get all those emails about cheap Viagra, amazing fat-fighting plant extracts, and attractive pillow-fighting college students. Yes, it's a chapter about spam—the email kind, not the canned meat kind. In these pages I'll tell you what it is, where it comes from, and what to do about it. It's the amazing, natural, and safe chapter about fighting spam! No dangerous stimulants or damaging side effects!

IN THIS CHAPTER

- What Is Spam?
- Why Does Spam Keep Coming?
- Specialty Spam
- Why Doesn't Someone Stop the Spammers?
- How Do Spammers Get My Email Address?
- The Damage Spam Can Do
- Reduce the Flow—10-minute Tactics to Reduce Spam
- Kill More Spam—In an Afternoon
- The Absolute Minimum

What Is Spam?

Despite its namesake, spam is not a favorite Hawaiian breakfast ingredient, a pig byproduct, or my dad's favorite lunch meat. That's SPAM, the compressed ham in a can made by the Hormel Foods Corporation.

No, spam is something completely different. And it's so important that it merits its own chapter in a computer security book. Lowercase *spam* is unsolicited commercial email or electronic junk mail.

It's those emails you receive in your inbox from people you don't know that advertise everything from religious T-shirts (see Figure 6.1) to adult websites (see Figure 6.2). Sometimes these ads are offensive. Other times they're stupid. Usually they are just plain annoying, especially because they arrive in huge volume and rarely do they advertise anything you need. Don't you think spam would be less annoying if it offered to sell you a freshly baked pecan pie or a tasty piece of haddock? Spam never advertises anything good.

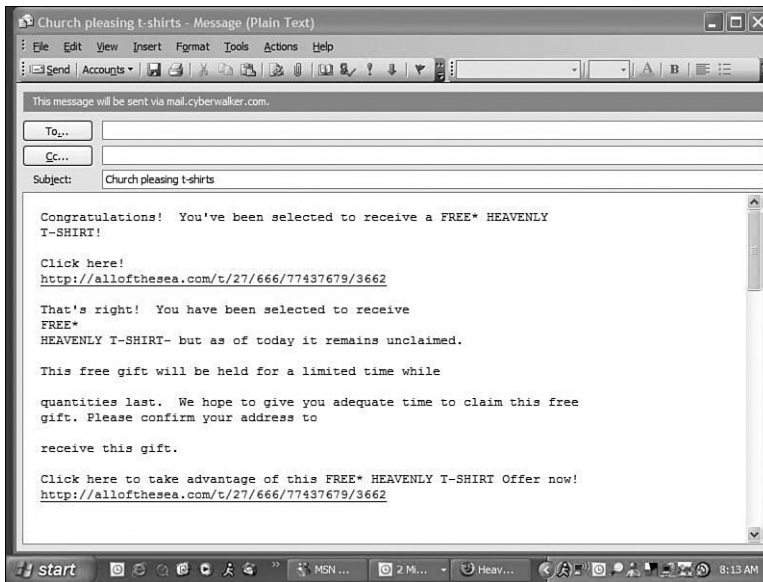
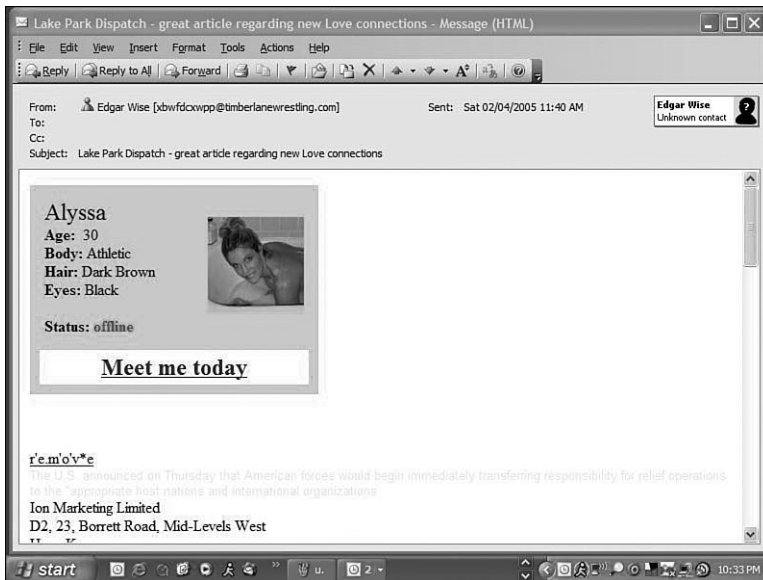


FIGURE 6.1

The site this spam links to offers a free "Wherever I go God is with me" T-shirt. It's odd, however, that the spammer has put 666 in the URL. Not a great marketing tactic when it comes to Christians.

**FIGURE 6.2**

This spam email features Alyssa, who has dark brown hair (isn't that blonde hair in the picture?) and black eyes (a little odd, too). Don't think she's interested in meeting you. The email clicks through to an adult website.

Why Does Spam Keep Coming?

Spam makes spammers money. It's hard to believe, but there are people out there who receive spam email, click the offer, and buy the advertised product. Now, you might think, why would anyone do that? Who knows, but they do because the spam keeps coming.

Personally, I think spam is perpetrated by people like that slightly evil kid in chess club. You know, the one who smelled vaguely sour and hiked his shorts too high in gym class. In reality, spammers are just business people—okay, slimy business people—bottom-feeding on yet another Internet opportunity.

caution Many reputable companies use email for legitimate marketing purposes. If you agree to receive email from an organization (that is to say, you opt-in), the email it sends you is not spam. If you find yourself in this situation, go back to the company's website and find out how to opt-out (unsubscribe). Most reputable companies have a mechanism that allows you to unsubscribe from their emails. Often, you'll find directions for unsubscribing at the bottom of the email in question.

Nevertheless, you don't need much more than Grade 9 math to figure out that if you send a lot of emails, a small percentage of the recipients read the email and an even smaller percentage buy the advertised product. Small as it is, it's income with a scaleable formula. If you can send millions of messages for the price of an Internet connection and a computer, you've got an almost free distribution system. And if it costs almost nothing to send and produces an income of any kind, it's profitable. So the spam keeps coming.

LOVELY SPAM, WONDERFUL SPAAAAAAM!

The origin of the term *spam* comes from a sketch by the British comedy troupe Monty Python. They did a bit on a restaurant that only featured dishes made with SPAM (note the uppercase), which is a canned ham product from Hormel. When the waitress describes items on the menu, a group of Vikings sing a song that goes something like "SPAM, SPAM, SPAM, SPAM. Lovely SPAM, lovely SPAM..." So spam was thus named because, like the song, it is an endless repetition of worthless text.

Specialty Spam

Spam distribution is a popular and effective way for Internet criminals to deliver their schemes or scams, however not all spam is made the same. Some custom spam techniques are used to for specific purposes or use distribution technologies outside of email. What follows are some curiosities in the specialty spam world.

Malware and Scam Distribution

Some bad guys use spam engines to send messages with attachments, which are actually viruses. When opened by unsuspecting recipients, the virus's payload turns the system into a zombie. A *zombie* is an infected computer that can be remotely controlled by a bad guy from the Internet to do bad things like send more spam or attack other computers by blasting nonsense data at them (often called a denial-of-service attack).

Spammers also use spam engines to distribute 419 scams and phishing emails.

tip If you want to learn what a 419 scam is and how to protect yourself against them, check out Chapter 5 "Identity Thieves and Phishers: Protect Your Good Name and Bank Account."

Hobbit Spam

In the spring and summer of 2006, some odd spam started to appear in inboxes. The messages contained lines from the JRR Tolkien's novel *The Hobbit*.

Here's an example:

"the hobbit that was lost. That only makes eleven (plus one mislaid) and not fourteen, unless wizards count differently to other people. But now please get on with the tale. Beorn did not show it more than he could."

Besides the bit of hobbit prose, the messages weren't pitching anything. So where did they come from? The theory is that a teenager (or similar inexperienced mischief maker) got his hands on a spam distribution tool and was taking it for a spin. Another theory is that a spammer was testing well-crafted prose against spam filters to see if he could fool them into letting the message through.

SPIM and Non-email Spam

Spam can also be unwanted, voluminous, and usually commercially motivated messages posted to web discussion forums, newsgroups, and blog comments.

There is also a spam variant that arrives in instant messenger (IM) programs. That kind of spam is sometimes referred to as SPIM.

SPIM looks like a chat message that usually has an embedded link of some sort or a file attachment. When you click on it, your system can be infected with some sort of malware. Sometimes the link takes you to a site that tries to sell you something.

The chatter that sends the SPIM can be someone unknown to you or you might recognize them. If they are a friend, colleague or family member, it could be that their system has been infected by a virus, which is using their identity to send SPIM.

If you receive a suspicious chat message, then message the person back and challenge them. Automated SPIMbots (programs that distribute spim) won't answer back. Friends, of course, will, unless their chat identity has been hijacked and is being used by a SPIMbot.

Good antivirus programs will detect spim, especially spim laden with malware, and alert you to the hazard.

Why Doesn't Someone Stop the Spammers?

Spammers are difficult to stop, partly because email as a technology is easy to use and hard to block. Each computer connected to the Internet has a unique numerical address called an Internet Protocol (IP) address. It's sort of like a telephone number. To send or receive information to or from a computer on the Internet, you have to know its IP address.

If a computer sends too much information—maybe too many spam emails—its IP address can be blocked by the recipient. This is what Internet service providers (ISPs) often do to curtail spam from a particular source. But if the owner of the sending computer changes the IP address, the ISP has to reblock the new address.

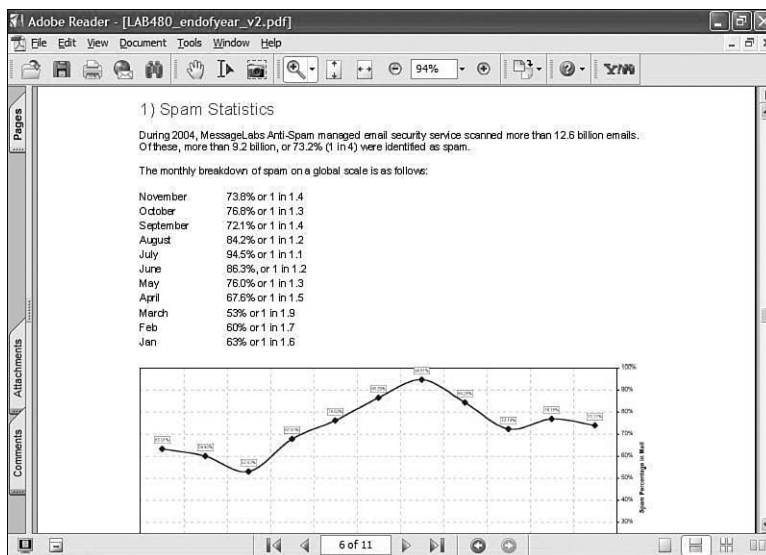
Because of this, spammers can evade being blocked by changing their IP address on a regular basis (or by sending from computers that they have hijacked and control through a botnet). They also move their operations overseas to countries that don't care or are more interested in making money than stopping spam.

Anti-spam laws have been enacted around the world in recent years by various countries, including the United States, to regulate commercial bulk email. Some high-profile spammers have been convicted but the laws have had little effect on reducing the total volume of spam. It keeps growing. However, spammers are being driven offshore to countries, such as China and Russia, where they are out of the grasp of anti-spam legislation.

According to a report by Message Labs, an email security company, the Australian Spam Act is one piece of legislation that has resulted in a “significant decrease in spam activity,” driving known spammers to shut down activities or go offshore. Still, the volume of spam continues to climb (see Figure 6.3).

note A botnet is a loose network of infected personal computers connected to the Internet that can be remote controlled by a bad guy (who wrote the malware that infected them). Internet criminals use botnets to distribute spam and attack target computers in denial of service attacks.

tip Get an intriguing handle on how much spam is out there and what malware or scams it is laden with on the Message Labs Intelligence web page at: <http://www.messagelabs.com/intelligence.aspx>

**FIGURE 6.3**

Email security company MessageLabs reported that spam constituted between 53% and 94.5% of email sent worldwide in 2004. Not much has changed; that volume is consistent today.

How Do Spammers Get My Email Address?

Spammers are a crafty bunch. They source email addresses wherever they can get their hands on them.

Website Harvesting

Programs are available that scan public address books on web-based email sites.

Spammers also have software that looks for email addresses embedded in websites. If you have a personal web page, an email address you post is almost guaranteed to be found by spammers. In fact, the people who receive the most spam tend to be webmasters. After emails are harvested they are compiled into lists and sold on the Internet.

Dictionary Spamming

There are also programs that combine random words and common names and pop them together in an effort to come up with valid email addresses.

With so many people using email, all the common names for email addresses such as Bob Smith are long gone at the big ISPs. So people make up their email addresses from common words. So let's say your ISP is called reallybigisp.com and your email address is topdog@reallybigisp.com.

Spammers might find you by running their dictionary program and combining the words *top* and *dog* together. They'll try sending an email to topdog@reallybigisp.com. They try this address combination against all the other major ISPs as well, so all the top dogs at aol.com, msn.com, and beyond get spam.

And don't think that becoming topdog1967@reallybigisp.com will help because after the spammers run through the most obvious words, they start combining them with numbers.

They'll even send email to aaaaaaa@reallybigisp.com, then aaaaaab@reallybigisp.com, then aaaaaac@reallybigisp.com, and so on.

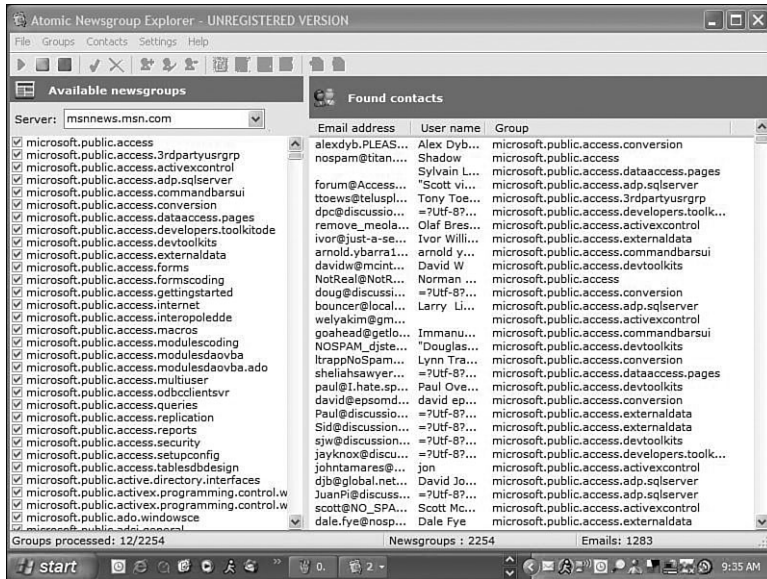
Because computers do all this work the spammers can try billions of combinations in hours. Then they spam to all these potential addresses. If they don't receive a bounced email from the address, they log it as valid and put it on their active list.

Commercial Email Lists

Millions of email addresses are available for sale via Internet download or on CD-ROM. Out of curiosity, I bought a list of 10 million Canadian email addresses for \$49. The company claimed they were all opt-in email addresses, meaning that the owners of the addresses had agreed to be put on the list. I found one of my addresses that is used for inbound mail only, however. It was never used to opt in to anything.

Newsgroups, Discussion Forums, and Interactive Websites

When you post your email address to the web to receive a newsletter or to sign up for a discussion forum, for example, you expose yourself to spammers. Email addresses can also be easily harvested from Internet-based discussion groups called newsgroups (see Figure 6.4) or discussion forums and the web at large. Some companies sell these lists of verified email addresses. Before making this information available, you might want to look for a privacy statement on the website to see what they are going to do with any personal information you give them. Credible websites stick to their privacy policies closely.

**FIGURE 6.4**

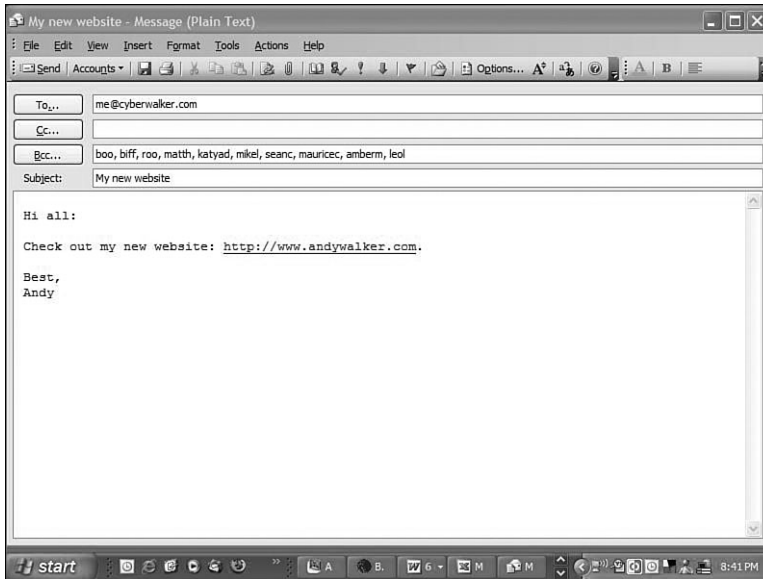
Atomic Newsgroup Explorer is a program that can extract thousands of email addresses and user names from Internet newsgroups in mere seconds. Here it has scanned the newsgroups at msnnews.msn.com.

Contests and Other Free Offerings

You can sign up to receive spam legitimately by entering contests or engaging in offers that appear to give you something for nothing. Oftentimes, these deals are email-harvesting schemes. Sometimes they even explicitly tell you in the fine print that you will receive bulk commercial email and you actually agree to this.

Email Forwarding

If you forward an email to dozens of people, make sure you send it to yourself in the To: field and put everyone else in the Bcc: field. Bcc means blind carbon copy. It's used to send a copy of the email to someone without revealing her email address (see Figure 6.5). If Bcc is not used, you expose everyone's email address to dozens of other people. It's been suggested that your email can be exposed to spammers that way. I know a few public relations people who have scooped my email for press release lists when another person has failed to hide my address in the Bcc field.

**FIGURE 6.5**

The Bcc: field is used when you want to send a copy of an email to someone, but hide her email address from others copied on the email.

Data Theft

Data is stolen from companies with alarming frequency. According to Privacyrights.org, as of December 4, 2007, 216,402,336 records containing sensitive personal information had been involved in security breaches since 2005 in the United States.

If you have ever registered your email with a company you do business with, and it is breached by a hacker, your email address could have been accessed and potentially sold by the perpetrators to spammers. Of course if that has happened, it is probably the least of your worries. This kind of data theft typically leads to identity theft or credit card fraud.

The Damage Spam Can Do

Spam might be free to send, but it is very costly to its recipients and the Internet community in the following ways:

- **It costs you money**—Spam costs millions of dollars a year in Internet

tip For a list of data breach incidents since 2005 and an updated number of records exposed by a security breach to date, see <http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total>

resources. It clogs Internet plumbing, forcing ISPs to buy bigger electronic pipes to carry all the information on the Internet. This drives up the cost of operations, which is passed on to you, the ISP's customer.

- **Wasted productivity**—If you're a business owner, spam wastes workers' time and productivity and increases expenses because it consumes helpdesk and IT resources to deal with it.
- **It wastes your time**—Spam wastes your time. Wading through spam to find the legitimate email takes time, especially if you get a lot of spam. If it takes you one second to delete a spam email and you get 900 spam emails each day (for a time I was getting more than 1,000), that wastes 15 minutes of your time.
- **It disconnects you**—If the flow of spam becomes too great, you have to abandon your email address in favor of a new one. This disconnects you from people who lose track of you because they don't update their email address lists.
- **It's annoying and offensive**—Spam is advertising you're not interested in, and that's just plain annoying. And often it comes with content that's offensive or at the very least distasteful.
- **It endangers children**—It exposes children to topics and images that they shouldn't have to worry about, including adult content.
- **It's a malware carrier**—Some spam carries email attachments that if opened can infect your computer with viruses or spyware. (Learn more about spyware in Chapter 2, "Spyware: Overrun by Advertisers, Hijackers, and Opportunists.")
- **It distributes scams**—Spam can also be used to mass-mail 419 scams or phishing emails. (Learn more about these scams in Chapter 5, "Identity Thieves and Phishers: Protect Your Good Name and Bank Account.")
- **It can get you kicked off the Net**—Some viruses can infect your computer so it turns into a spam-sending machine. And if your computer is identified as a source of spam, your Internet service provider may terminate your Internet account. Spammers use viruses to hijack other people's computers into sending spam because they create a

caution Be sure to run an up-to-date antivirus program on your computer to ensure your computer is not infected with a computer virus that has turned it into a spam distribution machine. Some viruses are engineered to install spam-sending software on a victim's computer.

massive network of spam-sending machines without worrying about having their own computers being identified as a spam sender. The spam also comes from thousands of computers and not just one, making it harder to stop.

Reduce the Flow—10-minute Tactics to Reduce Spam

You can do a few simple things to immediately reduce the flow of spam to your email address.

Don't Respond

First of all, never respond to spam. That means don't open spam, don't send angry responses to the spam sender, and definitely don't buy anything in a spam offer. If spam failed to work as an advertising medium, there would be little value in sending it. When you buy or respond to spam, you reinforce the notion that spam works as a marketing tool. And when you respond in any manner, you confirm that your email address is an active address. As a consequence, you'll receive more spam.

Don't Post Your Email Address on the Web

Don't give your main email address to anyone on the web. That's hard to do because many websites insist on your email address when signing up for their services. It's a good idea to maintain an alternate email address with Hotmail.com, Yahoo.com, Gmail.com, or any of the other free email services on the web. Check the secondary address occasionally to check for valid email, such as subscription confirmations, and if the volume of spam to that address gets to be too much, simply abandon it and get a new secondary address.

Webmasters Shouldn't Use mailto

If you run a website, don't post your primary email address to it using the HTML code called mailto.

A mailto link allows you to insert a link in a webpage that, when clicked, triggers the web surfer's email program and inserts the email address in the To field. A link that uses this technique looks like this:

```
Send me an email at <a href="mailto: me@mymailaddress.com">me@
mymailaddress.com</a>
```

Email harvester programs hunt for this code. Using a mailto is like wearing salmon-flavored socks at a cattery. You'll get bombarded with a lot of unwanted attention.

Instead, use the following JavaScript code, which achieves the same result but masks the email address. Be sure to customize the parts that say *me*, *example.com*, and *Link text* to your own needs.

```
<a href="email.html" onmouseover="this.href='mai' + 'lto:' + 'me' +  
▶ '@' + 'example.com'">Link text</a>
```

Learn more about this at www.december14.net/ways/js/nospam.shtml.

Turn Off Image Display in Email Programs

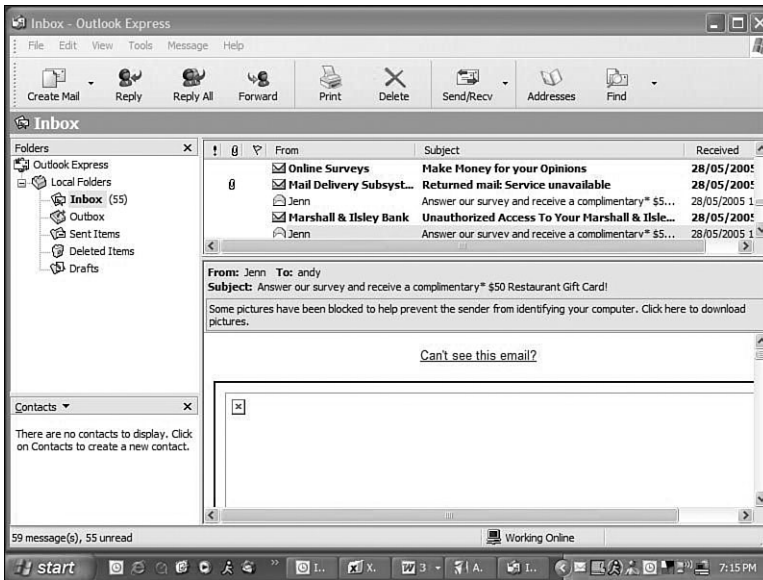
Both Outlook and Outlook Express have a feature that turns off images in HTML email. (HTML is a web programming language that is used to create web pages.) HTML email can include pictures, fancy fonts, and layout like a magazine. If you see a picture displayed in the body of an email, it was mostly likely created with HTML.

The ability to put images in email can cause an increase in spam. That's because spammers put an invisible pixel (an image of a transparent dot) in HTML emails. When an email is opened or previewed, the invisible pixel is fetched from the spammer's server. That tells the server that the email address affiliated with that image is a good one and is ripe to receive further spam.

Outlook 2003, Outlook 2007, Outlook Express 6, and Windows Mail (on Vista) have the ability to block these images from displaying (see Figure 6.6). Here's how to turn the features on in all these programs.

Outlook 2003

1. Click the Tools menu and choose Options.
2. Click the Security tab.
3. Under the Download Pictures heading, click Change Automatic Download Settings button.
4. Put a tick mark in the box marked Don't Download Pictures or Other Content Automatically in HTML Email.

**FIGURE 6.6**

Outlook Express 6 can block images from displaying in HTML emails when they are opened or in preview mode.

Outlook 2007

1. Click the Tools menu and choose Trust Center.
2. On the left side, click Automatic Download
3. Put a check mark in the box next to Don't Download Pictures Automatically in HTML Messages or RSS Items.
4. Look at the suboptions and consider if you want to allow those. If you use the Junk Email feature in Outlook, you might consider checking off the box next to Permit Downloads in Email Messages From Senders and to Recipients Defined in the Safe Senders and Safe Recipient Lists...

note This feature is built into Windows Mail in Vista, but in Windows XP it only works in Outlook Express 6 if you have installed Service Pack 2 (SP2), a major security add-on released by Microsoft in August 2004. You can install it by running Windows Update. Learn more about SP2 on **p. 274**.

Outlook Express 6/Windows Mail

1. Click the Tools menu and choose Options.
2. Click the Security tab.
3. Under the Download Images heading, put a check mark in the box marked Block Images and Other External Content in HTML Email (see Figure 6.8).

tip The image-blocking function in Outlook 2003/2007 and Outlook Express/Windows Mail has a nice side benefit. When porn-related spam arrives with graphic images of naked people doing surprisingly agile things, the images won't automatically display, saving you some shock and perhaps a little embarrassment if your grandma is nearby.



FIGURE 6.7

Outlook Express and Windows Mail has an image-blocking function to stop the display of embarrassing images and invisible tracking images.

Tweak Junk Mail Filtering on Your Mail Server

If your email provider allows you access to filter mechanisms on the mail server you should certainly tweak those filters to your liking. This is particularly useful if you have a vanity or company web domain and email addresses. This is like filtering junk mail at the post office before it gets put in the postman's delivery bag.

For example, I run the web site Cyberwalker.com and my company uses that domain (web address) for email. So on the server side of things I have access

to spam filtering. I log on to my provider, Everyone.net, and can tweak spam filter settings (see Figure 6.8).

You might want to call your Internet service provider (if they provide your email address) or the third-party company that hosts your email to see if you can access these settings.

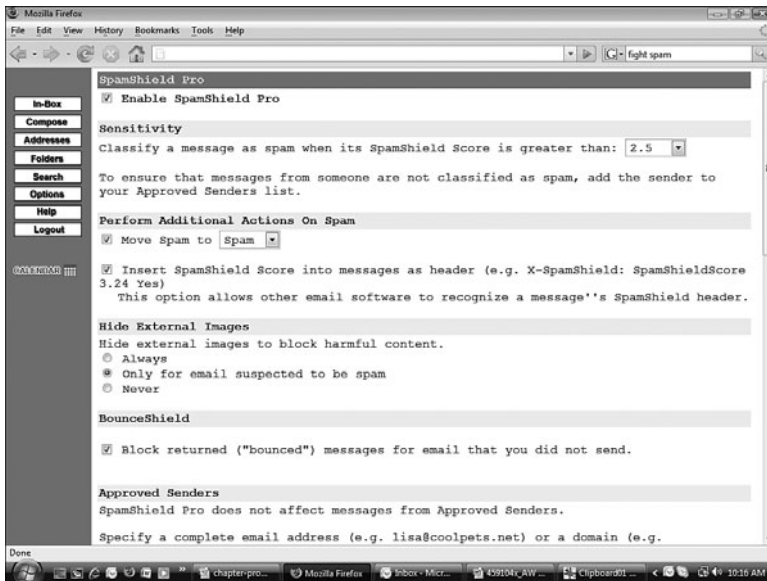


FIGURE 6.8

Some email providers, like Everyone.net, offer the ability to tweak spam filtering on the email server before it gets to your PC's email program.

Turn on Junk Mail Filtering

If you use Outlook 98, 2000, 2003, or 2007, turn on the Junk filter. It is not a foolproof method, but it stops much of the spam headed for your inbox.

Outlook 98, 2000, and 2002

To turn on the Junk filter, follow these steps:

1. In Outlook 98, click the Tools menu, and then click Organize.
2. Next, click Junk Email.
3. In the Automatically <action> Junk Messages list, select Move as the action, and then click to select the destination folder from the list. Click Turn On.

4. In the Automatically <action> Adult messages list, select Move as the action and then click to select the destination folder from the list. Click Turn On.

Outlook 2003 and 2007

Outlook 2003 and 2007 offer improved junk email tools over previous versions of Outlook. Here's how to turn the those features on:

1. Click the Tools menu and choose Options.
2. On the Preferences tab under Email, click Junk Email.
3. Select the level of protection you want (see Figure 6.9). If you receive a small volume of spam, choose Low. Note that High protection does a better job, but you will have to check your Junk email folder periodically to ensure that no legitimate emails have been mistakenly marked as spam.



FIGURE 6.9

Outlook 2003 (shown here) and Outlook 2007 offer vastly improved anti-spam tools over previous versions of the program, including conservative and aggressive sensitivity settings.

Kill More Spam—In an Afternoon

When you have a few hours to spare, here are a few more tactics to stop even more spam.

Install an Anti-Spam Program

Lots of anti-spam programs are available. All the big-name software security companies, including Symantec and McAfee, have their own. Choose one and install it; it will drastically reduce the flow of spam to your inbox.

I have had great success with Cloudmark Desktop (see Chapter 5, “Identity Thieves and Phishers: Protect Your Good Name and Bank Account,” for more on Cloudmark Desktop). It’s a plug-in for Outlook (see Figure 6.10), Outlook Express, and Mozilla Thunderbird that looks at each email as it comes in and electronically compares it to a database of spam email at Cloudmark. If a match is found, the email is marked as spam and is dumped into a spam folder or it can be automatically deleted; it’s your choice.

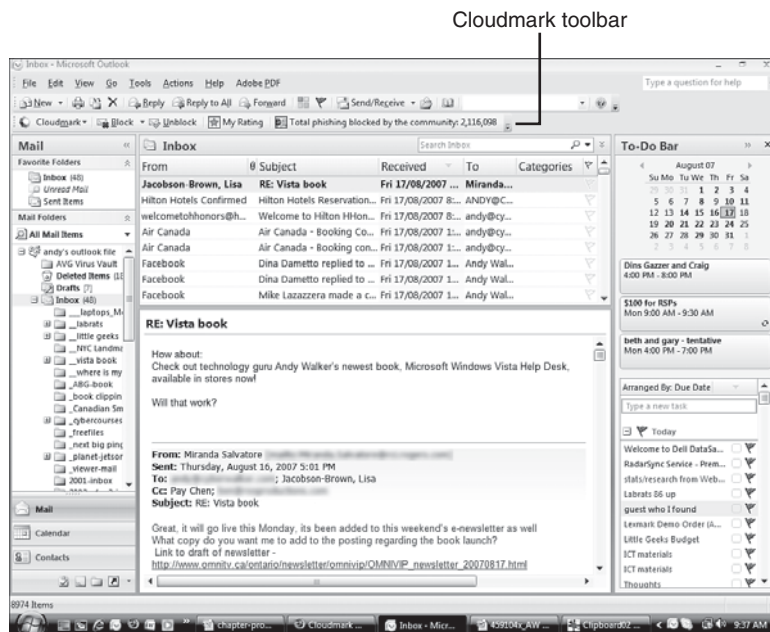


FIGURE 6.10

Cloudmark Desktop is a spam filter for Outlook, Outlook Express and Mozilla Thunderbird. It is shown here near the top of Outlook 2007.

The flaw in most anti-spam programs is that no matter how clever the detection engine, it will almost always misidentify some legitimate email as spam or let some spam through.

Cloudmark Desktop catches about 80%–90% of spam because humans look at each message. But fear not, there’s no team of spam spotters on the

Cloudmark staff looking at all your email. The program relies on its users. When email comes in, you can mark it as spam using the program. This reports the message as spam to the company's servers. If enough of us report the spam, a spam signature is generated and everyone that gets that spam in future has it filtered automatically by the software.

The community approach results in no false positives, which is lingo for a misidentification of a legitimate email as spam.

So if I get an email from my aunt who talks about the cocks crowing on her farm and the pretty tits singing in the trees outside her window, the Cloudmark software is not going to treat her email as spam, while others might because of misread keywords in her message.

Cloudmark Desktop costs \$39.95 per year, but it does have a free 30-day trial. It's available from www.cloudmark.com.

If you don't want to use Cloudmark Desktop, you might consider using Norton AntiSpam or McAfee SpamKiller, though I am no fan of either.

For the Mac, check out SpamSieve from <http://c-command.com/spamsieve/>.

A series of free anti-spam programs for Windows PCs are available for download at www.snapfiles.com/Freeware/comm/fwspam.html.

tip If you use a web-based email service such as Gmail.com, Hotmail.com, or Yahoo! Mail, it's worth investigating their built-in anti-spam features to set spam filtering sensitivity.

tip My pal Leo Laporte talks about his strategy for the Mac here: <http://techguylabs.com/radio/Main/StopSpam>

tip I've found that turning on Microsoft Outlook's built-in Junk Filter and installing Cloudmark Desktop helps blocks 99% of the spam that arrives in my inbox.

Fight Back!

If you are angry enough to fight back against spammers, here's how. Forward a message with your spam complaint to the ISP that hosts the spammer's email account. For example, if you received spam from bobby1234@llamasarenice.com, go to the website www.llamasarenice.com and look for a Contact Us page. Often ISPs have an email account called Abuse for such purposes. In this example, you'd send a copy of the spam to abuse@llamasarenice.com. You could also try postmaster@llamasarenice.com or hostmaster@llamasarenice.com. Try to verify what the correct address is first so you don't waste anyone's time.

The big problem with this solution is that ISPs are deluged by spam and to investigate every source of spam is not possible. Still, the option is available to you and it may make you feel better.

You can also use SpamCop.net (see Figure 6.11), a spam reporting service. It analyzes an email's content and header information (where it came from and how it got there). Then if it is deemed to be spam, it sends a warning to the ISP that provides the spammer with Internet service. ISPs tend to not like spammers on their network, so they often revoke service from them if they receive valid complaints. SpamCop.net has free and paid versions of its service.

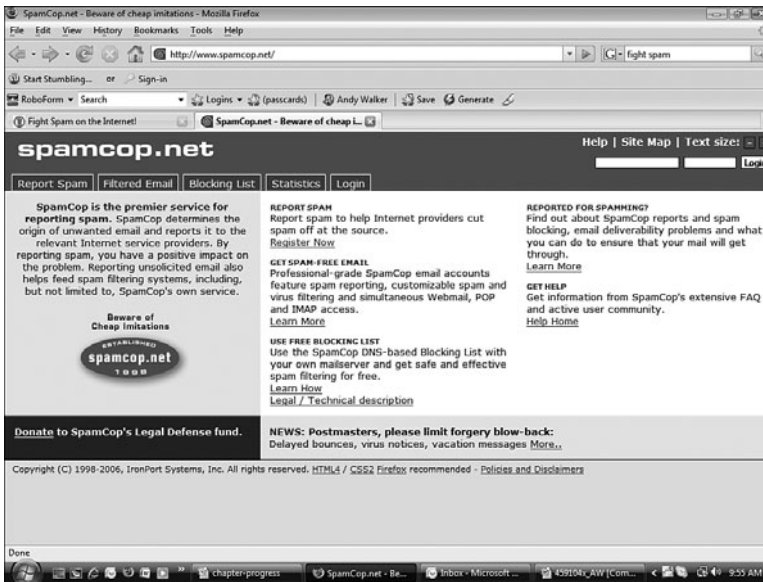


FIGURE 6.11

SpamCop.net analyzes your spam and reports it to the ISP that connects the spammer to the Internet.

More spam fight strategies are available here: <http://spam.abuse.net>

The Absolute Minimum

- Spam is unsolicited commercial email or electronic junk mail.
- SPAM is canned meat from Hormel.
- Spammers send massive volumes of email because they make money at it. Someone, somewhere, buys the products they advertise.

- Spam is an effective distribution method for scams and malware.
- A spammer's computer can be blocked but it's easy for him to evade this by changing his computer's IP address, the numerical address used to identify his computer on the Internet.
- Spam is free to send but costs recipients time, productivity, money, and aggravation.
- Never respond to spam.
- Never post your main email address to the web. Instead, use an alternate email for web forums, subscriptions, and the like.
- Use the junk mail filters in Outlook, Outlook Express, or Windows Mail.
- Install an anti-spam program. I recommend Cloudmark Desktop.
- Fight back by reporting spam to the spammer's ISP.

Index

NUMBERS

- 419 scams, 147
- 802.11 (wireless networks), 186

A

- ActiveX controls, defining, 332
- Ad-Aware 2007 Free anti-spyware program (Lavasoft), 392
- Admin accounts (Windows Vista)
 - creating, Windows Vista reinstallations, 311-312
 - passwords, 311
- administrator accounts (User Account Control), 44
- advanced fee fraud, 147
- advisory (security) websites, 346
- adware. *See also* pop-up windows
 - description of, 55
 - EULA warnings, 55
 - PUP, 56
- affiliate links (web pages), browser hijackers, 58
- alerts
 - Windows Defender, interpreting, 83-84
 - Windows Update, 154
- Anti-Phishing toolbar website (Netcraft), 339
- Anti-Phishing Working Group website, 141
- anti-rootkits, updating, 356
- anti-spam filters, 151
- anti-spam laws, 166
- anti-spam software
 - CA Anti-Spam 2007, 401
 - Cloudmark Desktop, 178-179, 399
 - Cloudmark website, 339
 - McAfee Internet Security Suite (Anti-Spam), 398
 - must-have features, 375
 - Spam Arrest, 400
 - SpamBayes, 401
 - SpamCop.net, 180
 - SpamSieve, 179

anti-spoofing software, 152-153

anti-spyware software

Ad-Aware 2007 Free (Lavasoft), 392

AVG Anti-Spyware Free Edition (Grisoft), 393

CA Anti-Spyware 2008, 396

cookie scans, 63

description of, 65

doubling up on, 74, 239, 319

downloading, 66

false positives, 249

Firefox web browser, 76

full system scans, 73-74, 82

inventory of, determining, 238

multiple programs, 74, 239, 319

must-have features, 373

quarantined items, removing, 248

recommended antispysware software list, 240

replacing, 246

Spy Sweeper (Webroot), 395

Spybot Search & Destroy, 66, 75, 392

Spyware Doctor (PC Tools), 396

status of, determining, 239

system scans, 247

updates, 239

phishing attack prevention, 153

signatures, 344-347

Windows Defender, 394

alert interpretation, 83-84

full system scans, 74, 82

quick system scans, 82

Real-time Protection feature, 76

removing spyware, 84

Windows Vista operation, 66

Windows XP operation, 67-70

Windows reinstallations, 281, 318-319

Windows Safe Mode, 84

antivirus software

AntiVir Personal Edition Classic (Avira), 389

AVAST! Home Edition, 387

installing, 246-247

virus scans, 247

AVG Anti-Virus Free Edition software (Grisoft), 35-38, 318, 345-346, 388

F-Secure Anti-Virus 2008, 391

failure updating, 27-28

false positives, 249

free trials, 34

freeware websites, 27

importance of, 25

installing, 34-37

inventory of, determining, 238

Kaspersky Anti-Virus 7.0, 391

Macs, 49

McAfee VirusScan Plus, 390

multiple programs, 239

must-have features, 372-373

NOD32 (Eset), 390

Norton AntiVirus (Symantec), 389

Panda Antivirus 2008, 391

quarantine areas, 27

quarantined items, removing, 248

recommended antivirus programs list, 240

replacing, 246
 spam, 171
 status of, determining, 238-239
 system scans, 24, 247
 updates, 37, 239
 failures, 27-28
 phishing attack prevention, 153
 virus signatures, 32-33, 344-346
 viruses
 removal, 26-27
 scans, 26, 38, 247
 signatures, 23, 32-33, 344-346
 web resources, 389
 Windows Defender, 247
 Windows reinstallations, 281, 318

AP (access points), dead-end Wi-Fi AP, 194-195

attachments (email), file extensions, 340

Australian Spam Act, 166

automatic Windows updates, 329, 355-356

AVAST! Home Edition antivirus software, 387

installing, 246-247
 virus scans, 247

AVG Anti-Spyware Free Edition anti-spyware program (Grisoft), 393

AVG Anti-Virus Free Edition software (Grisoft), 388

installing, 35-37, 318
 updating, 345-346

virus scans, 38, 349
 virus signature updates, 37

B

backdoor spyware. See Trojan horses

backups, 282

Documents folder (Windows Vista), 283-285
 Firefox web browser (Mozilla), 285
 games, 286
 Internet Explorer favorites/cookies, 285
 music, 286
 My Documents folder (Windows XP), 283-285
 Office 2003 (Microsoft), 286
 Outlook, 283
 Outlook Contacts, 288
 Outlook Express, 284
 pictures, 286
 video, 286
 virus removal, 253
 Windows Mail, 284
 Windows reinstallations
 Firefox web browser (Mozilla), 285
 games, 286
 Internet Explorer, 285
 music, 286
 Office 2003, 286
 Outlook, 283
 Outlook Contacts, 288
 Outlook Express, 284
 pictures, 286

video, 286

Windows Mail, 284

Windows Vista settings, 289-290

Windows XP settings, 289

WMP 10, 286

WMP 11, 287

Windows Vista settings, 289-290

Windows XP settings, 289

WMP 10, 286

WMP 11, 287

Bagle worm, description of, 16

bandwidth, stealing (wireless networks), 192

bank/credit statements, identity theft prevention, 158

Bcc field (email), spam attacks, 169

bills, paying, identity theft prevention, 137

BIOS

accessing, 293

Boot menu, 293

configuring, dangers of, 295

Bit Defender website, virus/software removal, 251

black-hat hackers, description of, 102.
See also hackers

Blacklight rootkit scanner (F-Secure), 95

Blaster worm, description of, 15

blocking images

Outlook, 173-174

Outlook Express, 173-175

bombs (viruses), description of, 7-9

Boot menu (BIOS), 293

boot sequences, Windows reinstallation, 292-294

boot viruses, effects of, 13

botnets, 8, 166

broadband Internet connections, Windows reinstallation, 323

browsers (web)

Firefox (Mozilla), 150

anti-spyware protection, 76

backups, 285

cleaning cookies, 80

downloading, 282

updating, 350

Windows reinstallation, 282, 321

hijackers, 8, 59. *See also* hackers; zombies

Cool Web Search website, 58

CWS shredder removal software, 268

description of, 57

HijackThis removal software,
260-268

web page affiliate links, 58

Internet Explorer

backups, 285

cleaning cookies, 79

Delete Browsing History dialog, 79

Protected mode, 77-78

C

CA Anti-Spam 2007 software, 401

CA Anti-Spyware 2008, 396

CA Internet Security Suite Plus, 384

Cabir virus, 49

cable

Internet connections, Windows reinstallation, 323

network cable, disconnecting from the Internet, 236

CDs

copy-protected CDs, recognizing, 90

Sony BMG rootkits, removing, 89

MediaMax, 92

XCP, 91

chats, SPIM, 165

chipset drivers, Windows reinstallation, 278

Cloudmark Desktop anti-spam software, 151, 178-179, 339, 399

Cohen, Dr. Fred, viruses, 5

Command column (System Configuration tool), 256

commercial email lists, spam attacks, 168

Comodo Free Firewall software, 397

configuring

BIOS, dangers of, 295

boot sequences, Windows reinstallation, 292-294

routers, wireless networks, 196-199

Windows Vista security

Ask Me Later option, 314

recommended settings, 313

update installations, 314

Connect to a Network dialog (Vista), wireless network connections, 191

Contacts (Outlook), backups, 288

contests (email), spam, 169

cookies

anti-spyware scanners, 63

cleaning, 62-63, 79-81

Internet Explorer, backups, 285

shopping websites, 62

spyware, 61-62

Cool Web Search website, browser hijackers, 58

copy-protected CDs, recognizing, 90

copying documents, identity theft prevention, 137

crackers, description of, 102. *See also* hackers

credit cards, identity theft prevention, 136-137

credit reports, identity theft prevention, 156

Australian websites, 158

Canadian websites, 157

U.K. websites, 157

U.S. websites, 157

credit/bank statements, identity theft prevention, 158

cutting/pasting web links, phishing attack prevention, 149

CWS (Cool Web Search) hijacks, description of, 58. *See also* browsers (web), hijackers

CWS shredder browser hijacker removal software, 268

D

daily security maintenance routines, updating

antispymware software signatures, 344-347

antivirus software signatures, 344-346

Data Execution Prevention (Security Center), 44-47

data theft, spam, 170

DDoS (Distributed Denial of Service) attacks, 8, 21, 104

deep scans (anti-spyware programs), 73-74, 82

Defender antispymware software (Windows), 247, 319

Delete Browsing History dialog (Internet Explorer), 79

deleting

cookies, 62-63, 79-81

hard drive partitions, 299-300

malware-related files/folders, 259

rootkits, 94

Blacklight rootkit scanner (F-Secure), 95

Malicious Software Removal Tool (Microsoft Windows), 96-97

MediaMax (Sony BMG rootkits), 92

Rootkit Hook Analyzer, 97

RootkitRevealer rootkit scanner, 95-96

System Restore, 98-100

XCP (Sony BMG rootkits), 91

desktop, Windows Vista reinstallations, 305-311

Device Manager, driver reinstallation, 314-315

DHCP (Dynamic Host Configuration Protocol), snooping attacks (wireless networks), 212-213

diagnostic mode, starting from Safe Mode, 244

dial-up Internet connections, Windows reinstallation, 323-324

dialers, description of, 59

dictionary spamming, 167-168

disabling

Data Execution Prevention (Security Center), 47

System Restore, 254

User Account Control (Security Center), 44

Wi-Fi adapters, 26

Windows Firewall, 113

Windows service malware

Windows Vista, 258

Windows XP, 259

discussion forums, spam attacks, 168

DNS (domain name servers), pharming attacks, 145

Documents folder (Windows Vista), backups, 283-285

DoS (Denial of Service) attacks, description of, 104

downloading

- anti-spyware programs, 66
- drive-by downloading, description of, 53
- drivers, 276-279
- files
 - dangers of, 53*
 - types to avoid, 54*
- Firefox web browser (Mozilla), 282

drivers

- chipset drivers, Windows reinstalls, 278
- defining, 275
- downloading, 276-279
- Ethernet drivers, 279-280
- INF (information) files, 278
- information searches, 280
- motherboard drivers, 278-279
- recovery discs, 277
- reinstalling
 - System Restore, 316-317*
 - Windows Vista, 315-316*
 - Windows XP, 314-316*
- troubleshooting, 316
- video drivers, 281
- Windows reinstalls
 - chipset drivers, 278*
 - Ethernet drivers, 279-280*

- motherboard drivers, 278*
- video drivers, 281*

droppers, definition of, 17

DSL Internet connections, Windows reinstallation, 323

E

email

- addresses, posting (spam attacks), 172
- attachments, file extensions, 340
- forwarding, spam attacks, 169
- junk mail filters, spam prevention, 175-176
- Nigerian 419 scams, 147
- Outlook, backups, 283
- Outlook Express, backups, 284
- phishing scams, 139-140
 - identifying, 141*
 - spoofing addresses, 141-142*
- spam, 162
 - anti-spam filters, 151*
 - anti-spam laws, 166*
 - anti-spam software, 178-179, 375, 398-401*
 - blocking, 166*
 - commercial email lists, 168*
 - contests, 169*
 - data theft, 170*
 - definition of, 151*
 - dictionary spamming, 167-168*
 - effects of, 170-172*
 - forwarding email, 169*

hobbit spam, 165
malware, 164
preventing, 171-180
reasons for, 163-164
responding to, 172
scam distribution, 164
SPIM, 165
spyware, 53
website harvesting, 167

unsubscribing, 163

Windows Mail, backups, 284

error messages, Safe Mode, 245

ESET Smart Security suite, 386

Ethernet drivers, 279-280

Ethernet ports

name/model numbers, determining, 279

NIC name/model numbers, determining, 280

EULA (End User License Agreements), adware warnings, 55

exploits (attacks), description of, 106

external hard drives, 276

F

F-Secure Anti-Virus 2008 software, 391

F-Secure Blacklight rootkit scanner, 95

F-Secure Internet Security suite, 383

F-Secure website, virus/software removal, 251

false positives (antivirus/antispyware programs), 249

favorites (Internet Explorer), backups, 285

Federal Trade Commission (FTC), filing complaints with, 138

File and Settings Transfer Wizard (Windows XP), backing up Windows XP settings, 289

file infector viruses, effects of, 13

file-sharing

dangers of, 53

wireless networks

security, 225

snooping attacks, 226-231

files

extensions, dangers of, 340

malware-related files, deleting, 259

searching by type, 291

filtering

MAC addresses, wireless networks, 208, 211

spam, 175-176

finding

files by types, 291

MAC addresses, wireless networks, 208-210

spyware information, 241-243

virus information, 241-243

Firefox web browser (Mozilla), 150

anti-spyware protection, 76

backups, 285

cookies, cleaning, 80

downloading, 282
 updating, 350
 Windows reinstallations, 282, 321

firewalls

Comodo Free Firewall, 397
 doubling up, 129
 FireWall Control (Vista), 109
 Firewall Plus firewall software (PC Tools), 126-127, 320, 398
 freeware, 113
 hardware firewalls, 107
 description of, 114
 installing, 129-130
 NAT, 114-115
 stateful inspection, 116
 installing, 120
 Firewall Plus software (PC Tools), 126-127
 Mac installations, 125
 two-way firewalls, 125-127
 must-have features, 374
 overview, 106-107
 Security Center (Windows), 40-41
 software, recommended attributes, 108
 SonicWall, 112
 third-party firewalls, features of, 110-112
 two-way firewalls, 125-127
 updating around, 345
 Windows Firewall
 disabling, 113
 launching, 123-124
 non-SP2 firewalls, activating, 125

overview, 108-109

SP2 firewalls, optional uses of, 124

Windows reinstallations, 282, 319-320
 wireless networks, turning on/off in, 219-220, 222
 ZoneAlarm Free, 397
 ZoneAlarm software website, 320-321

firmware, router updates, 356-358

folders, deleting malware-related files, 259

formatting, hard drive partitions, 300-302, 309-311

forums (discussion), spam attacks, 168

forwarding email, spam attacks, 169

freeware

anti-spyware software

Ad-Aware 2007 Free (Lavasoft), 392

AVG Anti-Spyware Free Edition (Grisoft), 393

Spybot Search & Destroy, 392

Windows Defender, 394

antivirus software

AntiVir Personal Edition Classic antivirus software (Avira), 389

Avast! Antivirus software (Alwil Software), 246-247, 387

AVG Anti-Virus Free Edition software (Grisoft), 35-38, 318, 345-346, 349, 388

websites, 27

FireWall Control (Vista), 109

firewalls, 113

gimpware, 368

open source software, 367

shareware, 369
source code, 367
trialware, 369
TweakUAC, 43, 337

full system scans (anti-spyware programs), 73-74, 82

G - H

games, backups, 286

gimpware, 368

Google.com website

driver information searches, 280
spyware information, finding, 241
virus information, finding, 241

GPS (Global Positioning Systems), wardrivers, 189

hackers

attacks

assessing damage, 120-121
detecting, 117
fixing, 119-122
logging, 118

black hats versus white hats, 102

DDoS (Distributed Denial of Service) attacks, 104

DoS (Denial of Service) attacks, 104

effects of, 103

hijacking, 103

identity theft, 103

motivations of, 105

overview, 102

personalities of, 102-103

spam generators, 104

targets of, 103-104

tools of, 105-106

web servers, 104

wireless hackers, 194

zombies, 104

hard drives

external hard drives, 276

installation files, Windows reinstallations, 273

partitioning, 297

deleting partitions, 299-300

formatting partitions, 300-302, 309-311

multiple partitions, 309

reformatting, 294

software activation, 304

System Recovery discs, 295

Windows Vista desktop installations, 305-311

Windows Vista installation discs, 304-311

Windows Vista installations, 311-313

Windows XP installation discs, 296-303

yearly security maintenance routines, 361

USB keys, 276

hardware firewalls, 107

harvesting websites, 167

hijackers (browsers), 8, 59. See also hackers; zombies

- Cool Web Search website, 58
- CWS shredder removal software, 268
- description of, 57
- HijackThis removal software, 260, 268
 - do-it-yourself course, 263-264*
 - F0, F1, F2, F3-IE Autoloading Programs from INI files, 266*
 - finding expert assistance, 262*
 - installing, 261*
 - Malware Removal forum, 263*
 - memory requirements, 264-265*
 - N0, N1, N2, N3, N4-Netscape/Mozilla Start and Search Page settings, 267*
 - O1-HOSTS file reductions, 267*
 - O2-Browser Helper Objects, 267*
 - O3-IE toolbars, 267*
 - O4-Autoloading programs, 268*
 - R0, R1, R2, R3-IE Start and Search Page web page addresses, 266*
- web page affiliate links, 58

hobbit spam, 165**home network routers, 184****home pages, browser hijackers, 57-59****HOSTS files, modifying, 28****HTML (Hypertext Markup Language)**

- link spoofing, 143
- mailto code, spam prevention, 172-173

ID, wireless network security

- router ID, changing, 217
- SSID, changing, 217-219

identity theft, 134

- hackers, 103
- phishing, 138
 - email scams, 139-140*
 - identifying, 141*
 - key loggers, 140*
- preventing
 - credit cards, 136-137*
 - credit reports, 156-158*
 - paper shredders, 136, 158*
 - paying bills, 137*
 - purses, 137*
 - reading credit/bank statements, 158*
 - Social Security numbers, 136*
 - wallets, 137*

recovering from, 137-138**signs of, 137****simple identity theft, description of, 134****skimming, description of, 135****techniques for, 134-135****web resources, 138****IM (instant messengers), SPIM, 165****images, blocking in**

- Outlook, 173-174
- Outlook Express, 173-175

Immunize feature (Spybot Search & Destroy anti-spyware program), 75

INF (information) files, drivers, 278

installation discs, Windows reinstallation, 276-277

Windows Vista reinstallation, 304-311

Windows XP reinstallation, 296

deleting hard drive partitions, 297-300

formatting hard drive partitions, 300-302

product keys, 302-303

installation files (hard drive), Windows reinstallation, 273

installing. See also reinstalling

antispymware software, 318-319

antivirus software, 34

AVAST! Home Edition, 246-247

AVG Free Edition, 35-37, 318

Windows reinstallation, 318

Firefox web browser (Mozilla), 321

firewalls, 120

Firewall Plus freeware (PC Tools), 126-127

hardware firewalls, 129-130

Macs, 125

two-way firewalls, 125, 127

Windows reinstallation, 319-320

HijackThis browser hijacker removal software, 261

SP2, 39, 221

updates, Windows Vista, 314

interactive websites, spam attacks, 168

Internet

broadband connections, Windows reinstallation, 323

cable connections, Windows reinstallation, 323

connection software, Windows reinstallation, 277

dial-up connections, Windows reinstallation, 323-324

disconnecting from

manual virus removal, 253

modems, 236

network cable, 236

reconnecting to, 240

routers, 236

spyware removal, 236-237, 253

USB adapters, 238

virus removal, 236-237, 253

Windows reinstallation, 291-292

wireless networks, 237

DSL connections, Windows reinstallation, 323

spyware information, finding, 241-243

virus information, finding, 241-243

Internet Explorer

cookies, cleaning, 79

Delete Browsing History dialog, 79

disadvantages of, 76

Protected mode, 77-78

security, recommendations for, 70

Internet Properties option (Security Center), 331-332, 335

IP addresses

addressing schemes, 115

spam, blocking, 166

ISP (Internet Service Providers), obtaining security software from, 374-375

J - K - L

- junk mail filters, spam prevention, 175-176
- KakWorm, description of, 6
- Kaspersky Anti-Virus 7.0 software, 391
- Kaspersky website, virus/spyware removal, 251
- Kazaa file-sharing program, dangers of, 53
- key loggers, 55
 - description of, 59
 - phishing scams, 140
- keys
 - product keys
 - Microsoft antipiracy techniques*, 308
 - recovering*, 273
 - Windows Vista reinstallations*, 273, 307
 - Windows XP reinstallations*, 273, 302-303
 - USB keys, 276
 - WEP keys, 200-201
- LAN cards. *See* Ethernet ports, 279
- legislation, anti-spam laws, 166
- license keys. *See* product keys
- Location column (System Configuration tool), 256
- logs, hacker attacks, 118
- LoveSan/Blaster worm, 16

M

- MAC addresses
 - spoofing attacks, 208
 - wireless networks
 - filtering in*, 208, 211
 - finding in*, 208-210
- macro viruses, 10
 - effects of, 11
 - Melissa, 7, 11
 - preventing, 12
- macros, definition of, 10
- Macs
 - antivirus programs, 49
 - firewalls, installing, 125
 - spyware, absence of, 64
 - viruses, overview, 48-49
 - wiping clean, 122
- mail servers, spam prevention, 175-176
- mailto HTML code, spam prevention, 172-173
- maintaining security**
 - daily routines, updating
 - antispymware software signatures*, 344-347
 - antivirus software signatures*, 344-346
 - monthly routines
 - network inspections*, 356
 - updating anti-rootkits*, 356
 - updating Office*, 358-360
 - updating router firmware*, 356-358

updating software, 360

updating Vista, 354-355

updating Windows XP, 353-356

weekly routines

Problem Reports and Solutions utility (Vista), 351

spyware scanning, 349

updating Firefox web browser, 350

virus scanning, 348-349

yearly routines, 361

Malicious Software Removal Tool (Microsoft Windows), rootkit removal, 96-97

malware

description of, 52

related files/folders, deleting, 259

rootkits

defining, 88-89

detecting, 92-93

operation of, 92-93

removing, 94-100

Russinovich, Mark, 90

Sony BMG, 89-92

uses for, 89

web resources, 92

Security Center (Windows), 41

signatures, updating, 246

spam, 164

Windows service malware, disabling, 258-259

Malware Protection section (Security Center), 238

Malware Removal forum (HijackThis browser hijacker removal software), 263

McAfee Internet Security Suite (Anti-Spam), 382, 398

McAfee VirusScan Plus antivirus software, 390

Mcafee.com website, 242, 250, 253

Media Sharing setting (Network and Sharing Center), wireless network security, 225

MediaMax (Sony BMG rootkits), removing, 92

Melissa macro virus, description of, 7, 11

memory

HijackThis browser hijacker removal software, 264-265

memory-resident viruses, 12-13

Microsoft website, virus/software removal, 251

Microsoft Windows Malicious Software Removal Tool, rootkit removal, 96-97

mobile gadgets, viruses, 49-50

modems, disconnecting from Internet, 236

monthly security maintenance routines, updating

anti-rootkits, 356

network inspections, 356

Office, 358-360

router firmware, 356-358

software, 360

Windows Vista, 354-355

Windows XP, 353-356

motherboard drivers, Windows re-installations, 278

motherboards, development of, 279

mouse, troubleshooting Windows XP
reinstallations, 302

movies, backups, 286

MP3 files, backups, 286

multi-partite viruses, 13-14

music

- backups, 286
- Sony BMG rootkits, 89
 - recognizing copy-protected CD*, 90
 - removing MediaMax*, 92
 - removing XCP*, 91

My Documents folder (Windows XP),
backups, 283-285

MyDoom worm, 16

Mytob worm, 16

N

naming computers, Windows Vista
reinstallations, 313

NAT (Network Address Translation)

- installing, 129-130
- overview, 114
- routers, 115
- stateful inspection, description of, 116

Netcraft Anti-Phishing toolbar website,
339

NetCraft phishing site blocker soft-
ware, 151

Netsky worm, 16

network adapters. *See* Ethernet ports

Network and Sharing Center (Vista),
wireless network security, 223-225

network cable, disconnecting from the
Internet, 236

Network Discovery setting (Network
and Sharing Center), 224-225

networks

- disconnecting from, 25
- home networks, 184
- inspections (monthly security mainte-
nance routines), 356
- VPN, wireless hackers, 194
- wireless networks
 - 802.11, 186
 - bandwidth stealing*, 192
 - damage from snooping attacks*,
187-188
 - dead-end Wi-Fi AP*, 194-195
 - detecting snooping attacks*, 212-213
 - disconnecting from the Internet*, 237
 - finding MAC addresses*, 208-210
 - MAC address filtering*, 208, 211
 - preventing snooping attacks*, 214-231
 - router configuration*, 196-199
 - security software*, 376
 - turning on/off access*, 214
 - turning on/off security measures*, 214
 - wardrivers*, 188-191
 - WEP activation*, 200-203
 - Wi-Fi*, 184
 - wi-phishing*, 193
 - wireless hackers*, 194
 - WPA activation*, 204-207

newsgroups, spam attacks, 168
NIC (Network Interface Cards),
279-280. *See also* Ethernet ports
Nigerian 419 scams, 147
NOD32 antivirus software (Eset), 390
Norton AntiVirus software (Symantec),
389
Norton Internet Security security suite
(Symantec), 381-382
NTFS (NT File Systems), 300
Nyxem/Mywife worm, 16

O

Office (Microsoft)
backups, 286
macro virus prevention, 12
updates, 338, 358-360
open source software, 367
Outlook (Microsoft)
backups, 283
Contacts, backups, 288
images, blocking, 173-174
junk mail filters, spam prevention, 176
Outlook Express
backups, 284
images, blocking, 173-175

P

P2P (Peer-to-Peer) programs, security,
22
Padobot/Korgo worm, 16
Panda Antivirus 2008 software, 391
Panda Internet Security suite, 386
paper shredders, identity theft preven-
tion, 136, 158
partitioning hard drives, 297
deleting partitions, 299-300
formatting partitions, 300-302,
309-311
multiple partitions, 309
passphrases (WPA), 205
Password-Protected Sharing setting
(Network and Sharing Center), wire-
less network security, 225
passwords
Admin accounts (Windows Vista), 311
Password-Protected Sharing setting
(Network and Sharing Center), 225
router passwords, 199, 217
paying bills, identity theft prevention,
137
payloads (viruses), description of, 7-9
payware, 366, 370
performance, troubleshooting, 64
phishing, 138
dangers of, 148
email scams, 139-141
key loggers, 140

pharming, 145

phones, 149

preventing

Anti-Phishing toolbar website (Netcraft), 339

anti-spam filters, 151

anti-spoofing software, 152-153

antispyware software updates, 153

antivirus software updates, 153

cutting/pasting web links, 149

direct phone communication, 149

Phishing tab (Windows Mail), 154-155

secure web pages, 150

site blocker software, 151

software updates, 154

risk assessments, 149

spoofing

email addresses, 141-142

link spoofing, 142-144

MAC addresses, 208

web addresses, 144

web links, 149

wi-phishing, 193

pictures, backups, 286

pop-up windows. See also adware

dangers of, 53

Windows Vista, managing in, 335

preventing

identity theft

credit cards, 136-137

credit reports, 156-158

paper shredders, 136, 158

paying bills, 137

purses, 137

reading credit/bank statements, 158

Social Security numbers, 136

wallets, 137

phishing attacks

anti-spam filters, 151

anti-spoofing software, 152-153

antispyware software updates, 153

antivirus software updates, 153

cutting/pasting web links, 149

direct phone communication, 149

Phishing tab (Windows Mail), 154-155

secure web pages, 150

site blocker software, 151

software updates, 154

snooping attacks (wireless networks)

changing default SSID, 217-219

changing router ID/passwords, 217

damage assessments, 214-215

file sharing, 226-231

firewall activation, 219-222

Network and Sharing Center (Vista) settings, 223-225

turning off UPnP, 222

turning on/off routers, 222-223

turning on/off security measures, 214

turning on/off wireless access, 214

spam

anti-spam software, 178-180

antivirus software, 171

image-blocking, 173-175

junk email filters, 175-176

mailto HTML code, 172-173

posting email addresses, 172

responding to, 172

Printer Sharing setting (Network and Sharing Center), wireless network security, 225

privacy, cookies effects on, 63

Private setting (Network and Sharing Center), wireless network security, 224

Problem Reports and Solutions utility (Vista), 351

processlibrary.com website, 265

product keys

Microsoft antipiracy techniques, 308

recovering, 273

Windows Vista reinstallations, 307

Windows XP reinstallations, 302-303

Protected mode (Internet Explorer 7), 77-78

Public Folder Sharing setting (Network and Sharing Center), wireless network security, 225

Public setting (Network and Sharing Center), wireless network security, 224

PUP (potentially unwanted programs), 56

purse contents, copying, identity theft prevention, 137

Q - R

quick system scans (anti-spyware programs), 82

ransomware, 8

Rbot worm, 16

Real-time Protection feature (Windows Defender), 76

recovery discs

drivers, downloading, 277

Windows reinstallations, 273, 277

reformatting hard drives, 294

software activation, 304

System Recovery discs, 295

Windows Vista

Admin account creation, 311-312

desktop installations, 305-311

installation discs, 304-311

naming computer, 313

product keys, 307

Windows XP installation discs, 296

deleting partitions, 297-300

formatting partitions, 300-302

product keys, 302-303

yearly security maintenance routines, 361

regedit, accessing, 11

Registry (Windows)

04-Autoloading programs, 268

remove changes from, 257

restoring changes in, 257

reinstalling. *See also* installing

drivers

System Restore, 316-317

Windows Vista, 315-316

Windows XP, 314-316

Windows Vista, 294

- activating Windows*, 337
- Admin account creation*, 311-312
- antispyware software*, 281, 318-319
- antivirus software*, 281, 318
- boot sequence configuration*, 292-294
- chipset drivers*, 278
- desktop installations*, 305-311
- disconnecting from the Internet*, 291-292
- driver reinstallation*, 315-316
- Ethernet drivers*, 279-280
- Firefox web browser (Mozilla)*, 282, 285, 321
- firewalls*, 282, 319-320
- formatting hard drive partitions*, 309-311
- game backups*, 286
- installation discs*, 272, 276-277, 304-311
- installation files (hard drive)*, 273
- Internet connections*, 277, 323-324
- Internet Explorer backups*, 285
- motherboard drivers*, 278
- music backups*, 286
- naming computer*, 313
- Office 2003 backups*, 286
- Office reinstallations (Microsoft)*, 338
- Outlook backups*, 283
- Outlook Contacts backups*, 288
- Outlook Express backups*, 284
- picture backups*, 286
- product keys*, 307
- recovery discs*, 273, 277
- Security Center*, 334-335

- security program updates*, 336-337
- settings backups*, 289-290
- software reinstallations*, 337-338
- SP1 service pack*, 274-275
- System Recovery discs*, 295
- System Restore*, 317
- tools for*, 272
- UAC*, 335-336
- validation*, 328-329
- video backups*, 286
- video drivers*, 281
- Windows Mail backups*, 284
- Windows Update*, 327
- WMP 11 backups*, 287
- yearly security maintenance routines*, 361

Windows XP, 294

- activating Windows*, 337
- antispyware software*, 281, 318-319
- antivirus software*, 281, 318
- Automatic Updates*, 329
- boot sequence configuration*, 292-294
- chipset drivers*, 278
- deleting hard drive partitions*, 297-300
- disconnecting from the Internet*, 291-292
- driver reinstallation*, 314-316
- Ethernet drivers*, 279-280
- Firefox web browser (Mozilla)*, 282, 285, 321
- firewalls*, 282, 319-320
- formatting hard drive partitions*, 300-302
- game backups*, 286

- installation discs*, 272, 276-277, 296-303
- installation files (hard drive)*, 273
- Internet connections*, 277, 323
- Internet Explorer backups*, 285
- motherboard drivers*, 278
- music backups*, 286
- Office 2003 backups*, 286
- Office reinstallations (Microsoft)*, 338
- Outlook backups*, 283
- Outlook Contacts backups*, 288
- Outlook Express backups*, 284
- picture backups*, 286
- product keys*, 302-303
- recovery discs*, 273, 277
- security*, 329-333
- Security Center*, 329-330
- security program updates*, 336-337
- settings backups*, 289
- software activation*, 304
- software reinstallations*, 337-338
- SP2 service pack*, 274, 333
- SP3 service pack*, 274-275
- System Recovery discs*, 295
- System Restore*, 316
- tools for*, 272
- troubleshooting mouse problems*, 302
- validation*, 327
- video backups*, 286
- video drivers*, 281
- Windows Mail backups*, 284
- Windows Update*, 325-326
- WMP 10 backups*, 286
- yearly security maintenance routines*, 361

removing

- rootkits, 94

- Blacklight rootkit scanner (F-Secure)*, 95

- Malicious Software Removal Tool (Microsoft Windows)*, 96-97

- MediaMax (Sony BMG rootkits)*, 92

- Rootkit Hook Analyzer*, 97

- RootkitRevealer rootkit scanner*, 95-96

- System Restore*, 98-100

- XCP (Sony BMG rootkits)*, 91

- spyware, 84

- resetting router ID/passwords (wireless networks)**, 217

- Rootkit Hook Analyzer**, 97

- RootkitRevealer rootkit scanner**, 95-96

rootkits

- anti-rootkits, updating, 356

- defining, 88-89, 106

- detecting, 92-93

- operation of, 92-93

- removing, 94

- Blacklight rootkit scanner (F-Secure)*, 95

- Malicious Software Removal Tool (Microsoft Windows)*, 96-97

- Rootkit Hook Analyzer*, 97

- RootkitRevealer rootkit scanner*, 95-96

- System Restore*, 98-100

- Russinovich, Mark, 90

- Sony BMG, 89

- recognizing copy-protected CD*, 90

- removing MediaMax*, 92

- removing XCP*, 91

UNIX, 89
 uses for, 89
 web resources, 92

routers. See also NAT (Network Address Translation)

firmware, updating, 356-358
 home network routers, 184
 IDs, 199, 217
 Internet, disconnecting from, 236
 NAT, 115
 passwords, 199, 217
 SSID, changing (wireless network security), 217-219
 Wi-Fi routers, 184
 wireless networks
 configuring for, 196-199
 security, 205
 turning on/off in, 222-223

S

Safe Mode (Windows), 84

accessing, 243-244
 diagnostic mode, starting, 244
 error messages in, 245
 manual virus removal, 255
 uses for, 245
 virus scans, 26

Safe Mode with Networking option, 244-245

antispyware programs, replacing, 246
 antivirus programs, replacing, 246
 system scans, 247

Sasser worm, 15-16

saved games, backups, 286

scanners

spyware scanners, 349
 virus scanners, 26, 38, 247, 348-349
 vulnerability scanners, description of, 105

search engines, 241-243

searches

Cool Web Search website, browser hijackers, 58
 files by type, 291

secure web pages, preventing phishing attacks, 150

security. See also Trojan horses; viruses; worms

anti-spam software

CA Anti-Spam 2007, 401
Cloudmark Desktop, 399
McAfee Internet Security Suite (Anti-Spam), 398
Spam Arrest, 400
SpamBayes, 401

anti-spyware software

Ad-Aware 2007 Free (Lavasoft), 392
AVG Anti-Spyware Free Edition (Grisoft), 393
CA Anti-Spyware 2008, 396
Spy Sweeper (Webroot), 395
Spybot Search & Destroy, 392
Spyware Doctor (PC Tools), 396
Windows Defender, 394

antivirus software, 387

AntiVir Personal Edition Classic (Avira), 389

Avast! Antivirus software (Alwil Software), 387

AVG Anti-Virus Free Edition software (Grisoft), 388

F-Secure Anti-Virus 2008, 391

Kaspersky Anti-Virus 7.0, 391

McAfee VirusScan Plus, 390

NOD32 (Eset), 390

Norton AntiVirus (Symantec), 389

Panda Antivirus 2008, 391

web resources, 389

firewalls

Comodo Free Firewall, 397

Firewall Plus (PC Tools), 398

ZoneAlarm Free, 397

Internet Explorer, recommendations for, 70

P2P programs, 22

security suites

CA Internet Security Suite Plus, 384

ESET Smart Security suite, 386

F-Secure Internet Security, 383

McAfee Internet Security, 382

Norton Internet Security (Symantec), 381-382

Panda Internet Security suite, 386

shopping tips, 381

Trend Micro Internet Security suite, 387

Webroot AntiVirus with AntiSpyware & Firewall, 384

ZoneAlarm Internet Security suite, 384-385

software

AVG Anti-Virus Free Edition, 35, 37-38

pros and cons of, 34-35

recommendations, 35

what not to do, 22-23

Windows Vista

Ask Me Later option, 314

recommended settings, 313

reinstallations, 334-337

update installations, 314

Windows XP reinstallations

Automatic Updates, 329, 332-333

Security Center, 329-330

security program updates, 336-337

Security Center

antivirus programs, determining status of, 238

automatic updates, 41

Data Execution Prevention, 44-47

firewalls, 40-41, 112

malware protection, 41, 238

User Account Control, 41-42

administrator accounts, 44

disabling, 44

managing, 43

standard user accounts, 44

triggering, 42

TweakUAC, 43

virus protection, 41

Windows Vista, 334-335

Windows XP, 329-332

seeding bots, 15. *See also* viruses

Service Packs (Windows), 273

Vista SP1, 274-275

Windows XP

*SP2, 39, 221, 273-274, 333**SP3, 274-275***services**turning off, manual virus removal,
257Windows service malware, disabling,
258-259**Services tab (System Configuration tool), manual virus removal, 256****shareware, 369****sharing files**

dangers of, 53

wireless network security, 225-231

shopping websites, cookies, 62**shredders (paper), identity theft prevention, 136, 158****signatures, updating**

antispymware software, 344-347

antivirus software, 344-346

malware, 246

spyware signatures, 72

viruses, 32-33, 37

simple identity theft, description of, 134**skimming, description of, 135****sniffers, description of, 105****snooping attacks (wireless networks)**

bandwidth stealing, 192

damage assessments, 214-215

damage from, 187-188

dead-end Wi-Fi AP, 194-195

detecting, 212-213

preventing

*changing default SSID, 217-219**changing router ID/passwords, 217**file sharing, 226-231**firewall activation, 219-222**Network and Sharing Center (Vista) settings, 223-225**turning on/off routers, 222-223**turning on/off security measures, 214**turning on/off UPnP, 222**turning on/off wireless access, 214*

wardrivers, 188-191

wi-phishing, 193

wireless hackers, 194

snoopware, description of, 56**social engineering, description of, 106****Social Security numbers, identity theft prevention, 136****software**

anti-spam software

*CA Anti-Spam 2007, 401**Cloudmark Desktop, 399**McAfee Internet Security Suite (Anti-Spam), 398**must-have features, 375**Spam Arrest, 400**SpamBayes, 401*

anti-spyware software

*Ad-Aware 2007 Free (Lavasoft), 392**AVG Anti-Spyware Free Edition (Grisoft), 393*

- CA Anti-Spyware 2008, 396
 - must-have features, 373
 - Spy Sweeper (Webroot), 395
 - Spybot Search & Destroy, 392
 - Spyware Doctor (PC Tools), 396
 - updating signatures, 344-347
 - Windows Defender, 394
 - Windows reinstallations, 281
- antivirus software
 - AntiVir Personal Edition Classic (Avira), 389
 - Avast! Antivirus software (Alwil Software), 387
 - AVG Anti-Virus Free Edition software (Grisoft), 388
 - F-Secure Anti-Virus 2008, 391
 - Kaspersky Anti-Virus 7.0, 391
 - McAfee VirusScan Plus, 390
 - must-have features, 372-373
 - NOD32 (Eset), 390
 - Norton AntiVirus (Symantec), 389
 - Panda Antivirus 2008, 391
 - updating signatures, 344-346
 - web resources, 389
 - Windows reinstallations, 281
- bad software, avoiding, 371-372
- firewalls, 107
 - Comodo Free Firewall, 397
 - Firewall Plus (PC Tools), 320, 398
 - must-have features, 374
 - recommended attributes, 108
 - Windows Firewall, 108-109
 - ZoneAlarm Free, 397
- freeware
 - gimpware, 368
 - open source software, 367
 - source code, 367
- installation discs, 276-277
- Internet connection software, Windows reinstallations, 277
- Microsoft antipiracy measures, 304
- payware, 366
- security
 - AVG Anti-Virus Free Edition, 35-38
 - obtaining software from ISP, 374-375
 - pros and cons of purchasing, 34-35
 - recommendations, 35
 - wireless networks, 376
- security suites
 - CA Internet Security Suite Plus, 384
 - ESET Smart Security suite, 386
 - F-Secure Internet Security, 383
 - McAfee Internet Security, 382
 - Norton Internet Security (Symantec), 381-382
 - Panda Internet Security suite, 386
 - shopping tips, 381
 - Trend Micro Internet Security suite, 387
 - Webroot AntiVirus with AntiSpyware & Firewall, 384
 - ZoneAlarm Internet Security suite, 384-385
- shareware, 369
- tips for buying, 370
- trialware, 369

- updating
 - monthly security maintenance routines*, 360
 - phishing attack prevention*, 154
- Windows Defender antispyware software, 319
- Windows reinstallations, 304
- ZoneAlarm firewall website, 320-321

SonicWall firewalls, 112

Sony BMG rootkits, removing, 89-92

Sophos.com website, 243

source code, freeware, 367

SP1 (Service Pack 1), Windows Vista, 274-275

SP2 (Service Pack 2), Windows XP, 39, 221, 273-274, 333

SP3 (Service Pack 2), Windows XP, 274-275

spam, 162

- anti-spam filters, 151
- anti-spam laws, 166
- anti-spam software, 178-179
 - CA Anti-Spam 2007*, 401
 - Cloudmark Desktop*, 399
 - McAfee Internet Security Suite (Anti-Spam)*, 398
 - must-have features*, 375
 - Spam Arrest*, 400
 - SpamBayes*, 401
- Australian Spam Act, 166
- blocking
 - images*, 173-175
 - IP addresses*, 166

- Cloudmark anti-spam software website, 339

- commercial email lists, 168

- contests, 169

- data theft, 170

- definition of, 151

- dictionary spamming, 167-168

- discussion forums, 168

- effects of, 170-172

- email addresses, posting, 172

- forwarding email, 169

- hobbit spam, 165

- junk email filters, 175-176

- mailto HTML code, 172-173

- malware, 164

- newsgroups, 168

- preventing, 172-180

- reasons for, 163-164

- responding to, 172

- scam distribution, 164

- sources of, 8, 104

- SPIM, 165

- spyware, 53

- websites, 167-168

Spam Arrest anti-spam software, 400

SpamBayes anti-spam software, 401

SpamCop.net anti-spam software, 180

SpamSieve anti-spam software, 179

SpectorSoft website, snoopware, 57

SPIM, 165

spoofing, 141

- anti-spoofing software, 152-153
- email addresses, 141-142
- link spoofing, 142-144
- MAC addresses, 208
- web addresses, 144
- web links, preventing, 149

Spoofstick anti-spoofing software, 153

Spy Sweeper (Webroot), 395

Spybot

- signatures, updating, 347
- spyware, scanning for, 349

Spybot Search & Destroy anti-spyware program, 66, 75, 392

spyware, 52

- adware. *See also* pop-up windows
 - EULA warnings, 55
 - PUP, 56

anti-spyware programs

- Ad-Aware 2007 Free (Lavasoft), 392*
- AVG Anti-Spyware Free Edition (Grisoft), 393*
- CA Anti-Spyware 2008, 396*
- description of, 65*
- doubling up on, 74*
- downloading, 66*
- false positives, 249*
- Firefox web browser, 76*
- full system scans, 73-74, 82*
- multiple programs, 319*
- must-have features, 373*
- quick system scans, 82*
- removing quarantined items, 248*

replacing programs, 246

Spy Sweeper (Webroot), 395

Spybot Search & Destroy, 66, 75, 392

Spyware Doctor (PC Tools), 396

updating, 153, 344-347

Windows Defender, 66-70, 74-76, 82-84, 394

Windows reinstallations, 318-319

Windows Safe Mode, 84

backdoor spyware. *See* Trojan horses

browser hijackers, 57-59

cookies, 61

anti-spyware scanners, 63

cleaning, 79-80

deleting, 62-63, 79-81

shopping websites, 62

dangers of, 52-53

definition of, 55

dialers, description of, 59

distributing, 9

downloading files

dangers of, 53

types to avoid, 54

drive-by downloading, description of, 53

effects of, 63

etymology of, 128

file-sharing, dangers of, 53

finding information on, 241-243

Internet Explorer

disadvantages of, 76

Protected mode, 77-78

security recommendations, 70

key loggers, 55, 59

Macs, 64

malware, description of, 52

pop-ups, 53. **See also** adware

removing, 251

antispymware tool updates, 239

determining antispymware status, 239

determining tool inventory, 238

diagnostic mode, 244

*disconnecting from the Internet,
236-237, 253*

multiple antispymware programs, 239

*recommended antispymware programs
list, 240*

reconnecting to the Internet, 240

Safe Mode, 243-245

*Safe Mode with Networking option,
244-245*

System Restore, 249-250

system scans, 247

removing manually

backups, 253

*disabling malware-related files/folders,
259*

disabling System Restore, 254

*disabling Windows service malware,
258-259*

disconnecting from the Internet, 253

research, 252

restarting Windows, 259

Safe Mode, 255

*startup program information website,
256*

System Configuration tool, 255-256

turning off services, 257

Windows Registry, 257

scanning for, Spybot, 349

signatures, updating, 72

snoopware, description of, 56

spam, 53

symptoms of, 64

top 10 nastiest spyware list, 60

Trojan horses, 60

web-surfing tips, 72

Windows Update, 72

Spyware Doctor (PC Tools), 396

SSID (routers), changing (wireless network security), 217-219

standard user accounts (User Account Control), 44

Start a New Transfer option (User Account Control), backing up Windows Vista settings, 290

startup program information website, manual virus removal, 256

stateful inspection, description of, 116

Storm Worm, 16

Symantec.com website, 242

virus/spyware removal, 250

virus/spyware threat analysis, 253

System Configuration tool

manual virus removal, 255-256

Services tab, 256

System recovery discs, Windows reinstallation, 295

System Restore

disabling, 254

driver reinstallation, 316-317

rootkit removal, 98-100
spyware removal, 249-250
virus removal, 249-250

T

TimeBombs, description of, 119. *See also* hackers

tombstone shopping, 149

Trend Micro Internet Security suite, 387

trialware, 369

Trojan horses, 60. *See also* viruses;
worms

description, 105
effects of, 18
overview, 16-17
versus viruses and worms, 9

troubleshooting

drivers, 316
mouse, Windows XP reinstallations,
302
performance, 64
spyware, 64
anti-spyware programs, 65-70, 74-75
cleaning cookies, 79-80
Firefox web browser, 76
full system scans, 73-74, 82
*Internet Explorer security recommenda-
tions*, 70
Protected mode (Internet Explorer 7),
77-78
quick system scans, 82
removing, 84

signature updates, 72
symptoms of, 64
web-surfing tips, 72
Windows Safe Mode, 84
Windows Update, 72

turning on/off

firewalls, wireless networks, 219-222
routers, wireless networks, 222-223
services, manual virus removal, 257
UAC (Windows Vista), 336
UPnP, wireless networks, 222
WEP, 200-203
wireless network security, 214
WPA, 204-207

tv shows, backups, 286

TweakUAC, 43, 337

two-way firewalls, installing, 125-127

U

**UAC (User Account Control), Windows
Vista**, 335

turning off, 336
TweakUAC tool website, 337

uninstalling rootkits, 94

Blacklight rootkit scanner (F-Secure),
95
Malicious Software Removal Tool
(Microsoft Windows), 96-97
MediaMax (Sony BMG rootkits), 92
Rootkit Hook Analyzer, 97
RootkitRevealer rootkit scanner, 95-96

System Restore, 98-100
 XCP (Sony BMG rootkits), 91

UNIX rootkits, 89

unsubscribing from email, 163

Update (Windows)

alerts, 154
 Windows Vista, starting in, 32
 Windows XP, starting in, 31

updates

anti-rootkits, 356
 antispyware software, 153, 239, 344-347
 antivirus software, 37, 153, 239, 344-346
 Firefox web browser (Mozilla), 350
 firewalls, 345
 malware signatures, 246
 Office (Microsoft), 338, 358-360
 router firmware, 356-358
 Security Center (Windows), automatic updates, 41
 software
 monthly security maintenance routines, 360
 phishing attack prevention, 154
 spyware signatures, 72
 viruses
 preventing, 31
 signatures, 32-33, 37
 Windows Update
 anti-spyware protection, 72
 Windows Vista reinstallations, 327
 Windows XP reinstallations, 325-326

Windows Vista
 automatic updates, 355-356
 reinstallations, 336-337
 security configuration, 314

Windows XP
 automatic updates, 329, 353-356
 reinstallations, 336-337

UPnP (universal plug-and-play), turning on/off in wireless networks, 222

USB adapters, disconnecting from Internet, 238

USB keys, 276

User Account Control (Security Center), 41

administrator accounts, 44
 disabling, 44
 managing, 43
 standard user accounts, 44
 Start a New Transfer option, backing up Windows Vista settings, 290
 triggering, 42
 TweakUAC, 43
 user accounts, 44

V

validation

Windows Vista, 328-329
 Windows XP, 327

variants (viruses), description of, 21

video

- backups, 286
- drivers, 281

viruses. See also Trojan horses; worms

- antivirus programs
 - failure updating, 27-28
 - false positives, 249
 - free trials, 34
 - importance of, 25
 - installing, 34-37, 246-247
 - must-have features, 372-373
 - removing quarantined items, 248
 - replacing, 246
 - signature updates, 37, 344-345
 - system scans, 24
 - updating, 153
 - virus scans, 38
 - virus signatures, 23
 - Windows reinstallations, 318
- authors of, 20-22
- boot viruses, effects of, 13
- botnets, 8
- Cabir, 49
- computer versus biological, 7
- DDoS attacks, 21
- definition of, 5, 105
- development of, 4
- disconnecting when infected, 25-26
- droppers, definition of, 17
- etymology of, 4-5
- file infector viruses, effects of, 13
- hijacking, 8

hoaxes, 18

- deleting files, 20
- effects of, 19
- identifying, 19-20

macro viruses, 10

- effects of, 11
- Melissa, 7, 11
- preventing, 12

Macs, effects on, 48-49

memory-resident viruses, 12-13

mobile gadget viruses, 49-50

multi-partite viruses, 13-14

payloads, description of, 7-9

preventing, Windows security updates, 31

ransomware, 8

removing, 26-27, 251

- antivirus tool updates, 239
- determining antivirus tool status, 239
- determining tool inventory, 238
- diagnostic mode, 244
- disconnecting from the Internet, 236-237, 253
- freeware websites, 27
- multiple antivirus tools, 239
- recommended antivirus programs list, 240
- reconnecting to the Internet, 240
- Safe Mode, 243-245
- Safe Mode with Networking option, 244-245
- System Restore, 249-250
- system scans, 247

removing manually

- backups, 253*
- deleting malware-related files/folders, 259*
- disabling Safe Mode, 255*
- disabling System Restore, 254*
- disabling Windows service malware, 258-259*
- disconnecting from the Internet, 253*
- research, 252*
- restarting Windows, 259*
- startup program information website, 256*
- System Configuration tool, 255-256*
- turning off services, 257*
- Windows Registry, 257*

scanning for, 26

- AVG Anti-Virus Free Edition software, 38*
- AVG Free Edition, 349*
- Windows Defender, 348*

Security Center (Windows), 39

- automatic updates, 41*
- Data Execution Prevention, 44-47*
- firewalls, 40-41*
- malware protection, 41*
- User Account Control, 41-44*
- virus protection, 41*

signature updates, 32-33, 37

SP2 (service pack 2), installing, 39

spam generators, 8

spreading, 6, 10

spyware, distributing, 9

symptoms of, 23

triggering, 5

Trojan horses versus, 9

variants, description of, 21

web resources, 241-243

what not to do, 22-23

Windows Vista antivirus strategies, 30

Windows XP antivirus strategies, 30

worms versus, 9

zombies, 164

Vista (Windows). *See* **Windows Vista von Neumann, John, viruses, 4**

VPN (virtual private networks), wireless hackers, 194

vulnerability scanners, description of, 105

W

wallet contents, copying (identity theft prevention), 137

warchalking, 189

wardialing, 189

wardrivers, 188-191

web addresses, spoofing, 144

web browsers. *See* **browsers (web)**

web links, spoofing, 142-144, 149

web pages

affiliate links, browser hijackers, 58

secure web pages, phishing attack prevention, 150

web resources, antivirus freeware, 389

web servers, 104

web-surfing antispysware tips, 72

Webroot AntiVirus with AntiSpyware & Firewall security suite, 384

websites

harvesting, 167

phishing site blocker software, 151

security advisories, 346

spam attacks, 168

virus hoax list, 19

weekly security maintenance routines

Problem Reports and Solutions utility (Vista), 351

spyware, scanning for, 349

updating, Firefox web browser, 350

viruses, scanning for, 348-349

WEP (Wired Equivalent Privacy)

keys, 200-201

turning on/off, 200-203

white-hat hackers, description of, 102

Wi-Fi (Wireless Fidelity), 184

802.11, 186

MAC addresses

filtering, 208, 211

finding, 208-210

routers, 184, 196-199

security software, 376

snooping attacks

bandwidth stealing, 192

changing default SSID, 217-219

changing router ID/passwords, 217

damage assessments, 214-215

damage from, 187-188

dead-end AP, 194-195

detecting, 212-213

file sharing, 226-231

firewall activation, 219-222

Network and Sharing Center (Vista) settings, 223-225

preventing, 214, 217-231

resetting router ID/passwords, 217

turning on/off routers, 222-223

turning on/off UPnP, 222

wardrivers, 188-191

wi-phishing, 193

wireless hackers, 194

turning on/off

access, 214

security measures, 214

WEP activation, 200-203

WPA activation, 204-207

Wi-Fi adapters, disabling, 26

Windows 95, finding MAC addresses for wireless networks, 210

Windows 98

file sharing, wireless network security, 228

MAC addresses, finding for wireless networks, 210

Windows Defender anti-spyware program, 66, 319, 394

alert interpretation table, 83-84

full system scans, 74, 82

quick system scans, 82

- Real-time Protection feature, 76
- removing spyware, 84
- signatures, updating, 346
- viruses, scanning for, 247, 348
- Windows Vista operation, 66
- Windows XP operation, 67-70

Windows Firewall. *See also* firewalls

- disabling, 113
- launching, 123-124
- non-SP2, activating, 125
- SP2, optional uses, 124

Windows Mail

- backups, 284
- Phishing tab, 154-155

Windows Me

- file sharing, wireless network security, 228
- MAC addresses, finding for wireless networks, 210

Windows product keys, 273

Windows Registry, 268

- remove changes from, 257
- restoring changes in, 257

Windows Safe Mode, 84

Windows security updates

- SP2, installing, 39
- viruses, preventing, 31

Windows Update

- alerts, 154
- anti-spyware protection, 72

Windows Vista

- reinstallations*, 327
- starting in*, 32

Windows XP

- reinstallations*, 325-326
- starting in*, 31

Windows Vista

- antivirus strategies, 30
- Connect to a Network dialog, wireless network connections, 191
- desktop installations, Windows Vista reinstallations, 309-311
- Documents folder backups, 283-285
- Ethernet ports, 280
- file sharing, wireless network security, 227, 231
- FireWall Control freeware, 109
- Immunize feature (Spybot Search & Destroy anti-spyware program), 75
- installation discs, Windows Vista reinstallations, 304-311
- Internet Explorer, Protected mode, 77-78
- MAC addresses, finding for wireless networks, 209
- Network and Sharing Center, 223-225
- pop-up windows, managing, 335
- Problem Reports and Solutions utility, 351
- reinstalling, 294
 - activating Windows*, 337
 - Admin account creation*, 311-312
 - antispyware software*, 281, 318-319

- antivirus software, 281, 318*
- boot sequence configuration, 292-294*
- chipset drivers, 278*
- desktop installations, 305-311*
- disconnecting from the Internet, 291-292*
- driver reinstallation, 315-316*
- Ethernet drivers, 279-280*
- Firefox web browser (Mozilla), 282, 285, 321*
- firewalls, 282, 319-320*
- formatting hard drive partitions, 309-311*
- game backups, 286*
- installation discs, 272, 276-277, 304-311*
- installation files (hard drive), 273*
- Internet connections, 277, 323-324*
- Internet Explorer backups, 285*
- motherboard drivers, 278*
- music backups, 286*
- naming computer, 313*
- Office 2003 backups, 286*
- Office reinstallations (Microsoft), 338*
- Outlook backups, 283*
- Outlook Contacts backups, 288*
- Outlook Express backups, 284*
- picture backups, 286*
- product keys, 307*
- recovery discs, 273, 277*
- security, 334-335*
- Security Center, 334-335*
- security program updates, 336-337*
- software reinstallations, 337-338*
- System Recovery discs, 295*
- System Restore, 317*
- tools for, 272*
- UAC, 335-336*
- validation, 328-329*
- video backups, 286*
- video drivers, 281*
- Vista settings backups, 289-290*
- Vista SP1 service pack, 274-275*
- Windows Mail backups, 284*
- Windows Update, 327*
- WMP 11 backups, 287*
- yearly security maintenance routines, 361*
- Safe Mode
 - accessing, 243-244*
 - error messages in, 245*
 - manual virus removal, 255*
 - starting diagnostic mode, 244*
 - uses for, 245*
- Safe Mode with Networking option, 244-245
 - replacing antispyware programs, 246*
 - replacing antivirus programs, 246*
 - system scans, 247*
- security
 - Ask Me Later option, 314*
 - recommended settings, 313*
 - update installations, 314*
- Security Center, 39, 334-335
 - accessing, 238*
 - automatic updates, 41*
 - Data Execution Prevention, 44-47*

- firewalls, 40-41, 112*
- Internet Properties option, 335*
- malware protection, 41*
- User Account Control, 41-44*
- services, disabling malware, 258
- settings backups, 289-290
- SP1 service pack, 274-275
- System Configuration tool
 - manual virus removal, 255-256*
 - Services tab, 256*
- System Restore
 - disabling, 254*
 - rootkit removal, 99*
 - virus removal, 249-250*
- UAC, 335
 - Start a New Transfer option, 290*
 - turning on/off, 336*
 - TweakUAC tool website, 337*
- updating, 354-355
- validation, 328-329
- Windows Defender operation, 66
- Windows Mail, Phishing tab, 154-155
- Windows Update
 - starting, 32*
 - Windows reinstallations, 327*
- wireless networks, firewall activation, 220

Windows XP

- antivirus strategies, 30
- Automatic Updates, 329
- Ethernet ports, determining name/model numbers, 279
- File and Settings Transfer Wizard, backing up Windows XP settings, 289

- file-sharing, wireless network security, 227-231
- installation discs, Windows XP reinstallations, 296-303
- MAC addresses, finding for wireless networks, 209-210
- My Documents folder, backups, 283-285
- reinstalling, 294
 - activating Windows, 337*
 - antispysware software, 281, 318-319*
 - antivirus software, 281, 318*
 - Automatic Updates, 329*
 - boot sequence configuration, 292-294*
 - chipset drivers, 278*
 - deleting hard drive partitions, 297-300*
 - disconnecting from the Internet, 291-292*
 - driver reinstallation, 314-316*
 - Ethernet drivers, 279-280*
 - Firefox web browser (Mozilla), 282, 285, 321*
 - firewalls, 282, 319-320*
 - formatting hard drive partitions, 300-302*
 - game backups, 286*
 - installation discs, 272, 276-277, 296-303*
 - installation files (hard drive), 273*
 - Internet connections, 277, 323*
 - Internet Explorer backups, 285*
 - motherboard drivers, 278*
 - music, 286*
 - Office 2003 backups, 286*

- Office reinstallations (Microsoft), 338*
- Outlook backups, 283*
- Outlook Contacts backups, 288*
- Outlook Express backups, 284*
- pictures, 286*
- product keys, 302-303*
- recovery discs, 273, 277*
- security, 329-333*
- Security Center, 329-330*
- security program updates, 336-337*
- settings backups, 289*
- software activation, 304*
- software reinstallations, 337-338*
- SP2 service pack, 274, 333*
- SP3 service pack, 274-275*
- System Recovery discs, 295*
- System Restore, 316*
- tools for, 272*
- troubleshooting mouse problems, 302*
- validation, 327*
- video, 286*
- video drivers, 281*
- Windows Mail backups, 284*
- Windows Update, 325-326*
- WMP 10 backups, 286*
- yearly security maintenance routines, 361*
- Safe Mode
 - accessing, 243*
 - error messages in, 245*
 - manual virus removal, 255*
 - starting diagnostic mode, 244*
 - uses for, 245*
- Safe Mode with Networking option, 244-245
 - replacing antispyware programs, 246*
 - replacing antivirus programs, 246*
 - system scans, 247*
- Security Center, 39, 329-330
 - accessing, 238*
 - Data Execution Prevention, 44-47*
 - firewalls, 40-41, 112*
 - Internet Properties option, 331-332*
 - virus protection, 41*
- service packs
 - SP2, 221, 274, 333*
 - SP3, 274-275*
- services, disabling malware, 259
- settings backups, 289
- System Configuration tool
 - manual virus removal, 255-256*
 - Services tab, 256*
- System Restore
 - disabling, 254*
 - rootkit removal, 99*
 - virus removal, 249-250*
- updating, 353-356
- validation, 327
- Windows Defender operation, 67-70
- Windows Update
 - starting, 31*
 - Windows reinstallations, 325-326*
- Wireless Network Connection Status dialog, 190
- wireless networks, firewall activation, 220

Wireless Network Connection Status dialog (Windows XP), 190**wireless networks, 184**

802.11, 186

Internet, disconnecting from, 237

MAC addresses

*filtering, 208, 211**finding in, 208-210*

routers

*configuring, 196-199**turning on/off, 222-223**Wi-Fi, 184*

security software, 376

snooping attacks

*bandwidth stealing, 192**changing default SSID, 217-219**changing router IP/passwords, 217**damage assessments, 214-215**damage from, 187-188**dead-end Wi-Fi AP, 194-195**detecting, 212-213**file sharing, 226-231**firewall activation, 219-222**Network and Sharing Center (Vista) settings, 223-225**preventing, 214, 217-231**resetting router IP/passwords, 217**turning on/off routers, 222-223**turning on/off UPnP, 222**wardrivers, 188-191**wi-phishing, 193**wireless hackers, 194*

turning on/off security measures, 214

WEP activation, 200-203

Wi-Fi, 184

WPA activation, 204-207

WMP (Windows Media Player), back-ups, 286-287**worms, 9, 14. See also Trojan horses; viruses**

Bagle worm, 16

Blaster worm, 15

description of, 105

effects of, 15

KakWorm, 6

LoveSan/Blaster, 16

MyDoom, 16

Mytob, 16

Netsky, 16

Nyxem/Mywife, 16

Padobot/Korgo, 16

Rbot, 16

Sasser, 15-16

Storm Worm, 16

WPA (Wi-Fi Protected Access)

passphrases, 205

turning on/off, 204-207

X - Y - Z**XCP (Sony BMG rootkits), removing, 91****XP (Windows). See Windows XP****XP SP2 service pack, 274, 333****XP SP3 service pack, 274-275**

454 **yearly security maintenance routines**

yearly security maintenance routines,
361

zombies, 104, 164

ZoneAlarm firewall software, 320-321,
397

ZoneAlarm Internet Security suite,
384-385