Windows LOCKDOWN!

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

que®

Andy Walker

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

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

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.

CHAPTER

6

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?

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.

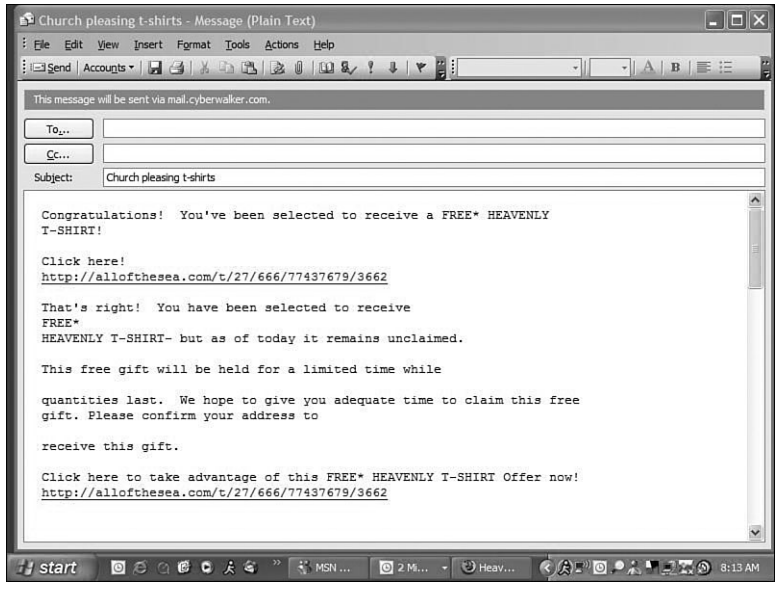

FIGURE 6.1

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.

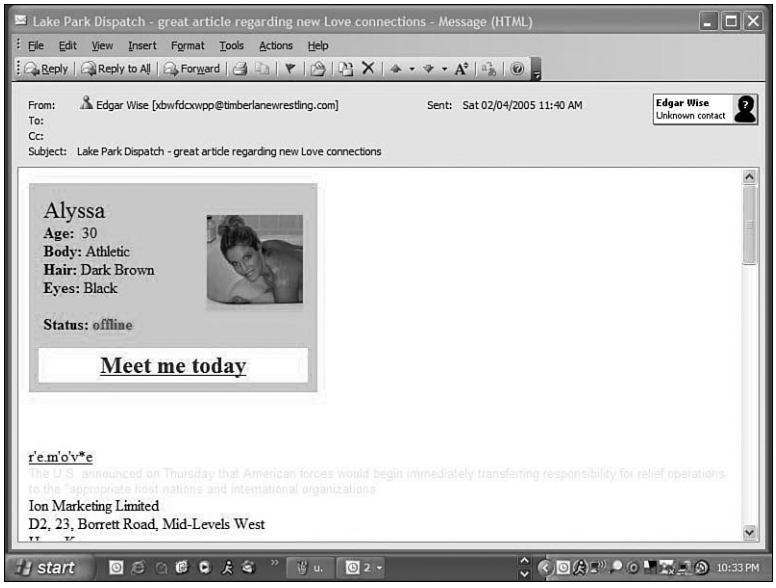

FIGURE 6.2

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.

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.

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).

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

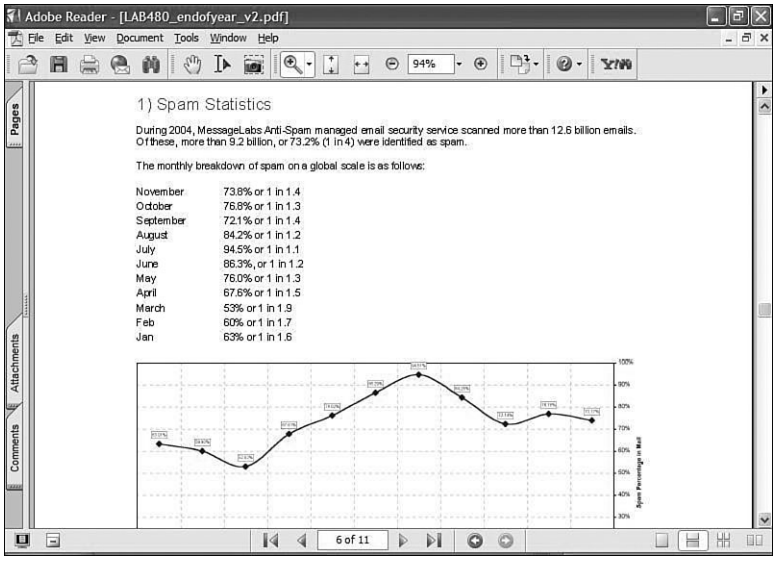

FIGURE 6.3

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.

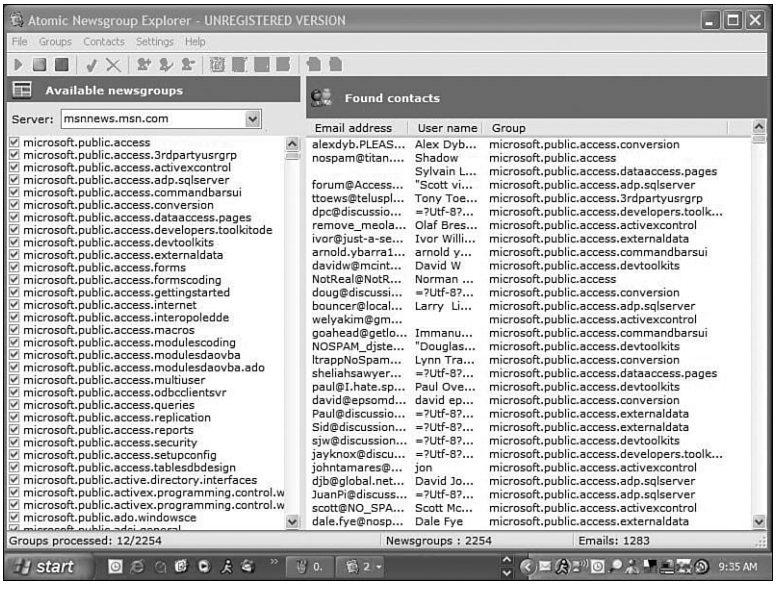

FIGURE 6.4

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.

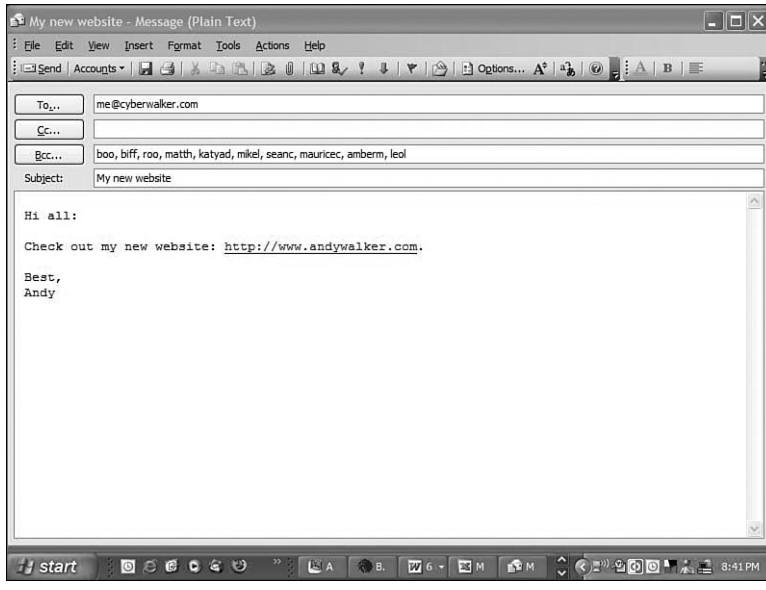

FIGURE 6.5

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.

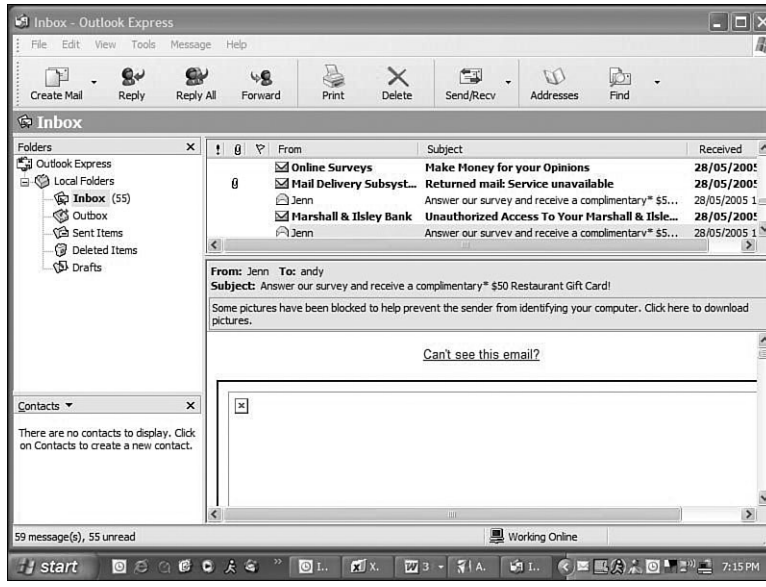

FIGURE 6.6

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.

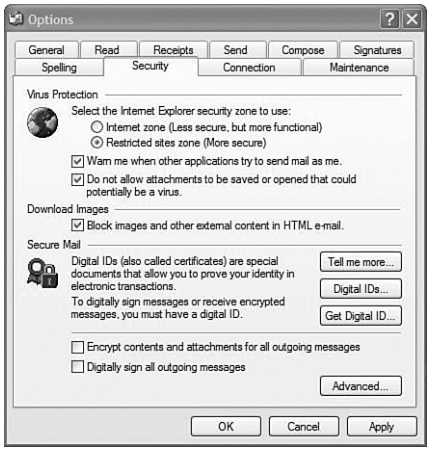

FIGURE 6.7

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.

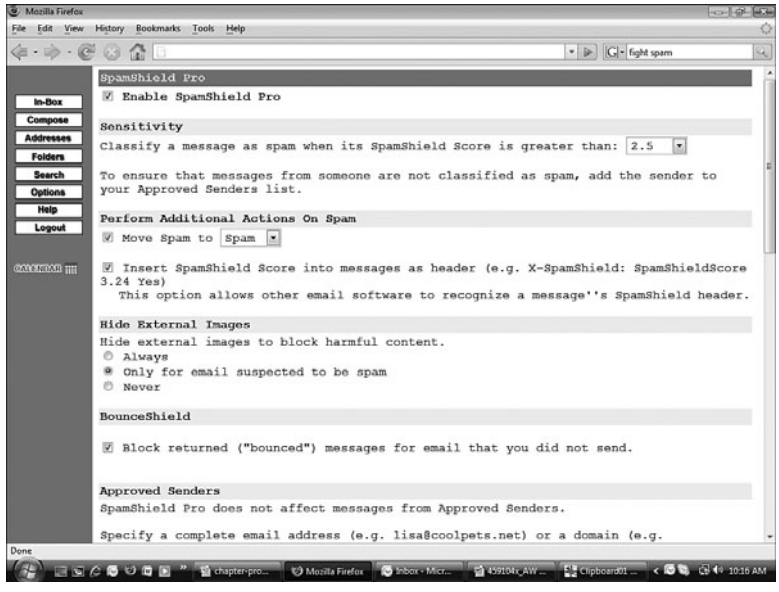

FIGURE 6.8

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.

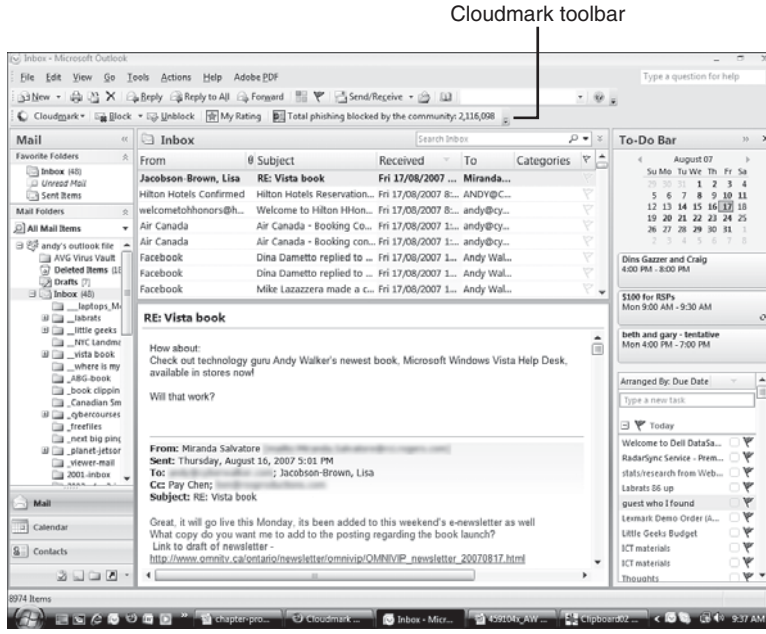

FIGURE 6.10

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.

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.

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.

Fight Back!

If youare 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.

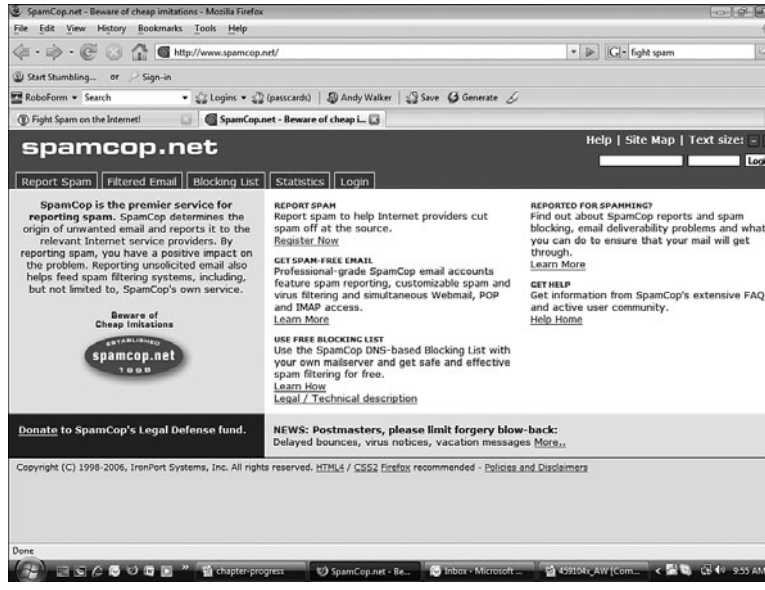

FIGURE 6.11

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

A

B

C

D

E

F

G - H

I

J - K - L

M

N

O

P

Q - R

S

T

U

V

W

X - Y - Z