OWN YOUR SPACE

Compliments of Microsoft®

KEEP YOURSELF AND YOUR STUFF SAFE ONLINE

Edited by Linda McCarthy and Denise Weldon-Siviy

Keep Yourself and Your Stuff Safe Online

Edited by Linda McCarthy and Denise Weldon-Siviy

page press
Smart Books for Smart People®

Publisher: Linda McCarthy
Editor in Chief: Denise Weldon-Siviy
Managing Editor: Linda McCarthy
Cover designer: Alan Clements
Cover artist: Nina Matsumoto
Interior artist: Heather Dixon
Web design: Eric Tindall and Ngenworks
Indexer: Joy Dean Lee
Interior design and composition: Kim Scott, Bumpy Design
Content distribution: Keith Watson

ISBN 978-0-615-37366-9
Library of Congress Cataloging-in-publication Data

McCarthy, Linda
Own your space : keep yourself and your stuff safe online / Linda McCarthy.
ISBN 978-0-615-37366-9 (electronic) 1. Computer security. 2. Computers and children. 3. Internet and teenagers. 4. Computer networks-Security measures. I. Title.

Visit us on the Web: www.100 pagepress.com

Download free electronic versions of the book from MySpace (http://www.myspace.com/ownyourspace) and Facebook (http://www.facebook.com/ownyourspace.net), and from Own Your Space (http://www.ownyourspace.net)

This book is dedicated to every teen who takes the time to learn about security and how to stay safe and be smart online. We also want to thank all of the teens joining this project and the teens who originally inspired this book—Eric and Douglas.

Table of Contents

Preface

Linda McCarthy was inspired to write the first edition of ***Own Your Space*** when the two teenagers in her house managed to destroy what she thought was a pretty darn secure home computer network. Linda was more inspired when she realized that Douglas and Eric weren't looking to break things or even trying to impress her when they brought down her home network. They were just using the Internet the way normal teenagers do.

Since then, this book has become a collaborative project to provide free security learning to teens and families online. Contributors to the 2010 edition include Denise Weldon-Siviy, a mother of four, teacher, and writer. Other experts we are adding to the team include specialists in firewalls, networking, and wireless systems, as well as advanced Mac and Firefox users. Our design specialists and anime artists tie these concepts together in teen friendly form. We also have several teens on the project and are adding new teens continually to keep the project current and fresh. Without that teen involvement, this book and project would not exist.

For now, and for later. Like malware, that changes every day, we plan to update this online version as needed to keep protecting our readers. Computer security is a moving target. The eBook format allows us to run along side.

It was very important to us that this book be made available to ALL teens and families in need of security learning. For that reason, this book is made available for free online under the Creative Commons Licensing (creativecommons.org).

This project is made available through corporate sponsors and would not be possible without their support.

Who This Book Is For

This is a book for every teen and an essential resource for every parent and teacher. Especially though, this is a book for the computer savvy, keyboard-comfy teens who use the Net every day and want to know how to secure their systems, preserve their Net lifestyles, and protect their data. This book provides important details to keep those teens, their privacy, their identities, and their reputations safe in cyberspace.

In short, this book is for normal teenagers—like you. We realize that you understand quite a bit about computers, probably a lot more than your parents. We also know from our own teens where the gaps in your computer knowledge tend to fall. We wrote this book to address those gaps.

Because we know your time is limited, we've kept this short and tried to focus on the important aspects of security. We also kept it interesting by including real examples and case studies from real teenagers just like you.

Even if you are a power user, this book is still for you! Sure, you'll know a number of the details we cover. Still, we are willing to bet that you'll find a number of details you weren't aware of before. And you'll certainly find a lot of detailed information you can share with a less enlightened friend, sibling, or parent.

Who This Book Is Still For, Just Not Quite 100% For

While this is a book full of details, it isn't a book full of numbered instructions. We wanted to write a book you'd want to sit down and read, not another 400-page technical manual. To any Mac users, we apologize for including only screenshots based on Windows 7. Much as we wanted to include all variations, that just wasn't practical for this edition. We will, however, be adding an appendix just for Mac users soon. Still, **most of this book applies every bit as much to Mac users as everyone else.**

What You'll Learn

This book is designed for any teen who is

- In fear of drive-by downloads of nasty adware, spyware, and viruses
- Anxious about scareware and ransomware
- Trying to stay safe on social networking sites
- Concerned about online predators and identity thieves
- Scattering secrets to the wind in favorite hot spots
- Shopping online without protection
- Unsure of the risks about webcams and sexting
- Dealing with cyberbullies at home or in school
- Blogging alone and in the dark

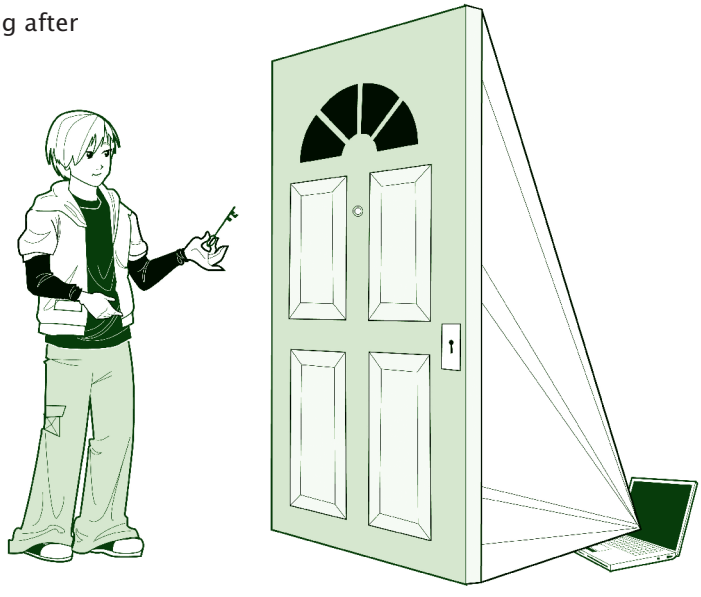
Got a thought? We've love to hear your feedback on this book. Just send it to lindamccarth@gmail.com.

Help save a forest and educate everyone in your school at the same time. Let your friends, family, and classmates know that this book is available for free on many corporate sponsor sites, as well as on MySpace (myspace.com/ownyourspace), Facebook (facebook.com/ownyourspace.net), and at Own Your Space (ownyourspace.net).

Chapter 1

Protect Your Turf

Braden is a typical 14-year-old. Over the past 6 months, he's grown three inches, gained four shoe sizes, and eaten his way through nearly a ton of pizza. He's also unintentionally trashed his family's computer no less than 12 times. First, he downloaded some cool emoticons to use with his IM messages. Those smiley faces came with embedded adware that overwhelmed him with pop-up ads and slowed down the speed of virtually everything. Then Braden installed a "free" video game that contained a Trojan program that let spammers in Russia take over his computer and use it to forward junk email. A few weeks later, Braden responded to what looked like a legitimate email asking him to confirm his Facebook login information. That phisher then used Braden's login to post links to adware to Braden's Facebook friends. Not long after that, Braden clicked **Yes** to install security software when a pop-up announced that his computer was infected with adware. As you've probably guessed, that software installed more adware. Braden's mom has spent so much time, and money, having the family computer fixed that she's beginning to wonder if the Internet is really worth the aggravation. What she is sure of is that Internet security has become a LOT more complicated than it used to be....



Since the Internet's inception in the late 1970s, the number of people who use the Net has doubled every 9 to 14 months. Do the math and you'll see a phenomenal growth chart—from 281 computers on the Internet in 1981 to a dazzling 400 million in 2000. By 2009, worldwide usage passed 1.5 billion **netizens**. Internet usage in the U.S. is nearing saturation levels.

Netizen A citizen of cyberspace (i.e. the Internet). A netizen is any person using the Internet to participate in online social communities. When you confirm a new friend on Facebook, you are expanding your online social group. You are being a good netizen!

While Internet usage among adults has risen steadily, Internet usage among teenagers has soared. As of June 2009, 90% of American teens lived in homes with Internet connections. If you're part of that 90%, it is especially important for you to understand how to protect your computer from nasty code.

As you'll learn later, your computer is at special risk. Adware sites target teenagers just like you by focusing their efforts on websites you and your peers tend to visit. Online forums are targeted by pedophiles posing as teens. Even identify theft, another potential consequence of nasty code, can be especially nasty for teenagers still in the process of defining their financial and business identities. If you use your parents' computers, you may also put their financial and personal information at risk.

For now, just keep in mind that there's a lot more to Internet security than running antivirus software. And, it's a lot more important than you probably realize. Over the next few chapters, we'll talk about what you need to know and do to help keep yourself, your computer, and maybe even your parents safer when using the Internet.

1.1 A Survey of Malware

Malware is a generic term for a piece of malicious code. That is, programming code specifically developed to harm a computer or its data. If you've studied Spanish (or Latin, for that matter), you'll know that "mal" means bad—like malcontent (an un-contented, unhappy person) or Darth Maul in *Star Wars Episode I* (the

obvious bad guy dressed in red and sporting horns). Nothing good ever starts with "mal." Malware is, quite literally, bad software.

Malware Programming code designed to harm a computer or its data.

Since malicious code and malware mean the same thing, for simplicity's sake we use the term malware throughout this book.

In the world of malware, there are several standard types of villains. We'll be covering all of these villains throughout the book, but the main categories are

- Viruses
- Worms
- Trojans
- Bot armies
- Keystroke loggers
- Spyware
- Adware
- Scareware
- Ransomware

You're probably already familiar with some of these categories. For instance, computer viruses are now so well-known in the popular culture that they provided the grand finale to the 1996 sci-fi thriller *Independence Day*. If you'll recall, Will Smith saved the day by helping Jeff Goldblum (better known as Ian Malcolm of *Jurassic Park*) to upload a computer virus to the "mother ship," disabling the alien space crafts' force fields. In real life, viruses and worms have taken out entire unprotected networks. In August 2009, attackers shut down Twitter for nearly three hours, leaving 44 million tweeters worldwide out of touch. If that doesn't sound like a big deal, imagine CNN or Fox News being driven off the air for an afternoon.

You are no doubt also familiar with antivirus software. Most, but not all, new computers now arrive fresh from the factory already preloaded with at least a trial version of one of the major antivirus packages. Usually, that's Norton AntiVirus, Trend Micro, McAfee, or Webroot. For virus protection, they are all excellent products.

You may not be aware, however, that antivirus software can't protect you against *all* types of attacks. Many people think as long as they have antivirus software installed that they are protected. That's not true because several layers of security are needed to protect you. Antivirus software is only one of those layers.

Before we take a look at the other layers of security, it is important to understand what antivirus software can and cannot do. Think of your antivirus software as a series of vaccinations. Having a polio vaccination won't keep you from getting hepatitis. Likewise, having antivirus software won't necessarily protect your computer from spyware or adware. In fact, if you don't routinely update your antivirus software, it may not even protect you from viruses. Like their biological cousins, computer viruses mutate. Just as you may need a new flu shot each winter to protect against new viral strains, you also need to update your antivirus software continuously. For other types of malware, you may need other types of protection. We'll explain these as we discuss the specific types of malware.

1.2 Protect Your Turf, Then Surf!

When you buy a computer, it is not secure. You should never pull a computer out of the box and connect it to the Internet unless you take steps to protect it. Think of your PC as a world traveler who needs vaccinations to avoid diseases in its travels.

In fact, your new computer most likely is plagued with numerous **security holes**, which are flaws in the way your computer's programs have been written that would make your computer vulnerable to attack. Just how serious the flaws in the code are determines how much access an attacker or that attacker's malware can gain.

Warning!

Uneducated programmers + programming mistakes = security holes!

If you're wondering why your computer has holes before you use it, the answer is that computer systems run on programs—literally tens of millions of lines of code that tell the computer how to interpret what you, the user, want to do. All those lines of code are written by human programmers. Those programmers can make mistakes that can be leveraged by hackers to gain unauthorized access to your computer. This probably sounds strange, but most programmers were never taught how to write secure code. To take it one step further, programmers don't think like criminals. We don't use that term very often, but that's what someone who deliberately steals or damages someone else's data is—a criminal. Your average programmer hasn't always thought, "Gee, I could use these lines of code to break into someone's computer," because the programmer doesn't actually WANT to break into anyone's computer.

Security Hole Any flaw in the way a computer program is written or used that makes your computer vulnerable to attack. Security experts also call this a security vulnerability.

The lack of focus on security as part of the design process is starting to change. More programmers are beginning to audit (double-check) their code with special tools that look for programming errors that can lead to unauthorized access to the system or data. It will take a long time for the programming community to catch up, however. Think of the millions of lines of code already out there that have been developed by programmers with good intent, but poor security-programming skills. Since all computer systems have security holes, you must protect yourself and patch those holes before you start surfing the Internet, downloading music, or gaming.

Warning!

Once connected to the Internet, an unprotected PC can fall victim to an attack in as little as 15 seconds! Protect your PC before you surf!

Why so fast? Once you're online, it can take as little as 15 seconds for someone to attack your machine. If you don't install security first, that first attacker may gain access to your computer without you even knowing about it! At worst, the attacker

could make off with enough personal data to steal your identity. If you use financial software to track the bank account you opened for college savings when you picked up that after school job, keep in mind that your data isn't just information. It could be cash as well. And just to add another twist, a hacker could even use your computer to launch an attack on other computers! For these reasons (and many more we'll get to later), don't ever surf the Internet without security patches, antivirus software, and a firewall installed.

When you bought your computer, you probably started with a list of requirements: how much memory, how much disk space, what kind of graphics you'd need for your favorite games, whether you want to burn DVDs as well as view them. Before you go online, you also need a Computer Security shopping list. This list is a basic list. You should not leave any one of these items off your list. Virus protection **must** be on that list. You have to install it and configure it to update your computer automatically. You also need to install any security patches that have been issued for the operating system and the software you plan to use.

Security Patch A fix to a program to close a known security hole. Patches are routinely issued for operating systems (like Windows 7) and Internet browsers (like Internet Explorer and Firefox) as well as other software applications.

The Internet is an infinitely cool place, but so is the vampire royal court in Volterra. We think it would be great to actually visit such a place, but only if we understood the Volturi laws, knew about Aro and Jane's gifts in advance, and also brought our own immortals. The Internet is exactly like that! There are wonderful, new, and exciting things going on there—but you really shouldn't show up without knowing the risks, understanding how to defend yourself, and arming yourself with the right protection.

Chapter 2

Know Your Villains

Meet Eric, from Novato, California, a normal teen who likes to create web pages for his friends. Eric spends a lot of time on the Internet. He is a major gamer, visits a lot of different sites looking for ideas, and likes to download free software.

Before Eric got his own laptop, he used his mom's computer to surf the Net and download free stuff. Eventually, Eric's mom's computer became so slow that it took *forever* to download software. That's when Eric asked a friend what to do. That's also when Eric found out that he should have had a firewall and downloaded patches to prevent hackers from planting spyware on his system. Eric thought that antivirus software was all he needed and he hadn't even heard of drive-by malware.

Eric found out the hard way that a hacker had back-doored his system and had been sifting confidential information from it. Well, not really Eric's system. It was his mom's system and her confidential information. Oops... sorry, Mom. Now, Eric has his own laptop with a firewall, current patches, antivirus software, and spyware protection.

What happened to Eric? He simply didn't have the right protection to keep the bad guys out and to keep malware from getting in. Like most teens, he needed to know a lot more about security than he did. While virus protection is important, it's not the be-all and end-all of security. Malware can land on your system in *many* ways. You might simply have visited a website that was created specifically to download malware.

2.1 Why Does Malware Exist?

When you consider the work that goes into writing software, you have to ask why anyone would care that much about trashing a stranger's computer system. To understand why people write malware, it helps to look first at WHO is doing the writing.

A surprising number of teens write malware. According to Sarah Gordon, a research scientist, their most common feature is that they don't really have a lot in common. Sarah's research finds that malware writers "vary in age, income level, location, social/peer interaction, educational level, likes, dislikes and manner of communication."

While some teens write malware for the sheer challenge of it, others have heavy delusions of grandeur. That was certainly the goal of Sven Jaschan, an 18-year-old German teen sentenced in 2005 for creating Sasser.e, a variation on an earlier worm dubbed Netsky. Sasser literally bombarded machines worldwide with millions of junk emails. Jaschan's goal wasn't so much to disrupt Internet commerce as it was to make a name for himself. After his arrest, he told officials he'd only wanted to see his "creation" written about in all the world's papers. Jaschan told reporters, "It was just great how Netsky began to spread, and I was the hero of my class."

Is this admiration justified? Rarely. Consider the case of Jeffrey Lee Parson, of Minnesota, an 18-year-old arrested for releasing a variant of the Blaster virus. While his friends and neighbors were taken in, at least briefly, the world of computing professionals was not. Parson had simply copied the existing Blaster code, created a simple variant (no real skill there), then was almost immediately caught when he released it. Not a lot to admire.

The nature of malware writers has evolved with the technology they exploit. The very first self-replicating programs existed mostly as technical exercises. For the most part, these were generated by graduate school programmers, often as research for doctoral theses. Early on, the field expanded to include teens looking for a technical challenge as well as the stereotypical loner geeks—socially awkward teens using malware to make names for themselves. These writers not only didn't hide their viruses very well, many didn't hide them at all. Their goal was to make as many people as possible aware of what they'd done.

Not surprisingly, many of these malware writers were caught. Even today, some malware includes "authorship" information. In some cases, those really are the names of the malware writers or the groups they represent. In other cases, named authors are themselves additional victims.

More recently, professionals are joining the loop. Mikko Hypponen of the Finnish security firm F-Secure, notes, "We used to be fighting kids and teenagers writing viruses just for kicks. Now most of the big outbreaks are professional operations." They're looking for cash, not infamy.

People still write malware for the challenge or to become famous, but they also write malware to steal intellectual property from corporations, destroy corporate data, promote fraudulent activity, spy on other countries, create networks of compromised systems, and so on. Malware writers know that millions of computer systems are vulnerable and they're determined to exploit those vulnerabilities. Does this mean that all those teen users are turning into computer criminals? No. It simply means that with widespread Internet access, more people are using the Internet to commit crimes.

Wanted Dead or Alive!

Reminiscent of old West bounties, a few malware victims have struck back by offering substantial awards for the capture and conviction of worm and virus writers. Microsoft began the trend, offering $250,000 bounties, and then upping the ante to $500,000 on the Blaster and SoBig authors. Preparing for future attacks, on November 5, 2003 Microsoft funded the Anti-Virus Reward Program with $5 million in seed money to help law enforcement agencies round up malware writers. That approach continues today. In February 2009, Microsoft offered a $250,000 reward for information leading to the arrest and conviction of those responsible for the Conficker worm.

More information than ever is now stored on computers, and that information has a lot of value. You may not realize it, but your computer and your data are at higher risk than ever before. Even if your machine contains NO personal information, NO financial data, and nothing that could be of the slightest interest to anyone, your computer could still be used to attack someone else's. As Justin, a 16-year-old from Atherton, California said, "It's just not right that someone can take over my machine and use it."

2.2 Viruses

A computer virus is a set of computer instructions that self replicate. A virus can be a complete program (a file to itself) or a piece of code—just part of a computer program file. In its most basic form, a virus makes copies of itself.

Virus Number 1

Fred Cohen, then a doctoral student at the University of Southern California, wrote the first documented computer virus in 1983 as an experiment to study computer security. Officials were so concerned, they banned similar projects!

Some viruses are designed to spread only in certain circumstances, like on a certain date, or if the machine belongs to a certain domain.

Some viruses also carry a payload. The payload tells the virus to do damage like delete files or attack other systems. We'll talk more about payloads in the next section.

Even a virus without a payload can cause major problems. Just through the process of making copies of itself, a virus can quickly use up all available memory in your computer. This can slow your computer down to a pathetic crawl and sometimes prevent other programs from running altogether.

A **computer virus** is very much like a biological virus. The flu is a good example of a biological virus that can be transmitted from one person to another. Just how sick you get depends on the type of flu and whether you've been vaccinated. Once you're infected with the flu, you can also spread that virus to every person you come in contact with.

In the worst-case scenario, you could be another Typhoid Mary. As you probably know, Mary Mallon was an immigrant cook working in New York at the turn

of the 20th century. Apparently healthy herself, from 1900 to 1915 Mary spread typhoid fever around town along with her signature peach desserts. Records tell us that she infected between 25 and 50 people and probably caused at least 3 deaths. After the 3rd death, "Typhoid Mary" was placed in quarantine for the rest of her life. In the computer world, carriers have a much larger reach. While Typhoid Mary infected a mere 50 people during a span of 15 years, computer viruses and worms can infect thousands of other systems in just minutes. When Code Red was unleashed in 2001, it infected more than 250,000 systems in only 9 hours.

Virus A piece of code that makes copies of itself. A virus sometimes also includes a destructive payload.

Once a single computer is infected with a virus, it can infect hundreds of thousands of other computers. Just how much damage occurs depends on two things: (1) whether each computer in the chain is protected with current antivirus software, and (2) whether the virus carries a payload. If the virus carries a payload, it may perform harmful requests such as deleting all your data; if it does this, it can't continue to replicate because there are no programs for it to infect. Most viruses don't contain a payload; they simply replicate. While this sounds harmless enough, the copying process uses memory and disk space. This leaves affected computers running slowly, and sometimes not at all.

2.2.1 How Viruses Replicate

Most viruses require human intervention to start replicating. You may inadvertently trigger a virus to begin replicating when you click on an infected email attachment. Once a virus is activated, it can create and distribute copies of itself through email or other programs.

Your machine can be infected by a virus if you:

- Share infected CDs
- Download and run infected software from the Internet
- Open infected email attachments
- Open infected files on a USB drive

Just as the flu reappears each winter with just enough variations to negate last year's flu shot, computer viruses keep coming back as new variants. Often, just a few simple tweaks to the code creates a new variant of the virus. The more variants that are created, the more opportunities a virus can have to get access to your system. McAfee reports that over 200 new viruses, Trojans, and other threats emerge *every day*.

When physicians check for a physical virus, they rely on a set of symptoms that together indicate the presence of that virus. Some antivirus programs use a signature to identify known viruses. You can think of the signature as a fingerprint. When crime scene investigators (CSIs) want to know whether a particular criminal's been on the scene, they check for that person's fingerprints. When antivirus software wants to know whether your machine's been infected with a particular virus, it looks for that virus **signature**.

Signature A unique pattern of bits that antivirus software uses to identify a virus.

2.2.2 Malicious Payloads

All viruses are annoying. Some also have a destructive payload. A payload is a subset of instructions that usually does something nasty to your computer system—or someone else's. The payload may destroy or change your data, change your system settings, or send out your confidential information. The damage can be costly.

Where Do Viruses Come From?

Geographically, viruses are awfully diverse. Some of the more well-known malware actually originated in some pretty unexpected places:

- Brain originated in Pakistan.
- Chernobyl, while referring to a Ukrainian city, originated in Taiwan.
- Michelangelo began in Sweden, not Italy.
- Tequila sounds Mexican, but originated in Switzerland.
- Yankee Doodle, surprisingly, really is an American virus!

When the Chernobyl virus payload was first triggered in 1999, nearly a million computers were affected in Korea alone, costing Korean users an estimated quarter of a *billion* dollars!

A payload commonly used today initiates a denial of service (DoS) attack. This type of attack is usually aimed at a third-party website and attempts to prevent legitimate users from gaining access to that website by literally flooding the site with bogus connections from infected machines. MyDoom.F is a good example of a piece of malware with a destructive payload. MyDoom.F carries a payload that initiates a denial of service attack AND deletes picture files and documents from your PC. More damaging payloads can modify data without even being detected. By the time the deadly payload has been discovered—it's simply too late.

While we tend to think of viruses as attacking programs, they most often infect documents or data files. Unlike programs, which users rarely share indiscriminately, documents travel far and wide. During the writing of this book, the document that contains this chapter traveled between Linda, Denise, the publisher, reviewers, and typesetting. Other documents are FAR more widely traveled. Job seekers may distribute hundreds of resumes via email or upload in search of that perfect position.

2.2.3 Virus Hall of Shame

There are literally tens of thousands of computer viruses. Some are nasty, others funny, still more just annoying. Of the field, we found these viruses to be worthy of note:

Famous Viruses

Virus Name	Release Date	Significance
Stoned	1987	If political activism were a category of virus, Stoned would be its first member. Usually benign, it displayed the message: "Your PC is now stoned! LEGALIZE MARIJUANA!"
Yankee Doodle	1989	This virus serenaded its victims by sending part of the tune "Yankee Doodle" to the system speakers every day at 5 pm.

continues

Famous Viruses *continued*

Virus Name	Release Date	Significance
Michelangelo	1991	This was the disaster that never happened. This virus was designed to delete user data on the trigger date, March 6—Michelangelo's birthday. WIDELY reported in the press, doom-sayers prepped the world for up to 5 million affected machines. March 6 came and went with fewer than 10,000 incidents. What Michelangelo actually accomplished was to make the average computer user aware of computer viruses and to spur massive sales of antivirus software.
Concept	1995	Spread through word processing documents, this virus was one of the first to work on multiple operating systems.
Marburg	1998	Named after Marburg hemorrhagic fever, a nasty form of the Ebola virus that causes bleeding from the eyes and other body openings. The Marburg virus triggered three months (to the hour) after it infected a machine. Random operating system errors followed. Marburg also compromised antivirus products, putting the victim at risk from other viruses.
CH1	1998	Named for the Ukrainian nuclear reactor that imploded in 1986, this family of viruses actually originated in South-East Asia. When the virus triggered on the 26th of the month, it rendered the PC unable to boot AND overwrote the hard drive with garbage characters.
Waledec	2009	Also known as the Valentine's Day virus, targets receive an email from a "secret admirer" with a link to a "Valentine" site. That site actually downloads a program that not only co-opts the target's address list to replicate itself, but installs a bogus antivirus program calling itself MS AntiSpyware 2009. The rogue antivirus program issues repeated warnings that the user's computer is being used to send SPAM, then demands that the user register and purchase the latest version to remove the "virus."

You'll note that many of these viruses are more historic than current. If you're wondering whether viruses are out of vogue, hardly! What's actually happened is that malware has advanced with technology. Old viruses evolve into new viruses (called variants or mutations), and new viruses are being created every day. Many of those viruses now include features of worms, Trojans, and other forms of more advanced malware. The viruses are still there—they're just playing with meaner friends.

You'll also notice that much of the last table is written in past tense. We talk about these viruses as if they no longer exist. That's not technically true. Viruses are a bit like socks that get lost in the washing machine. They have a way of reappearing. Most of these viruses still exist in the wild corners of cyberspace. They're just no longer major threats. That's partly because some of these viruses target technology that's no longer in use. A bigger factor, however, is that antivirus software now routinely searches for them. The truly dangerous viruses at any moment are the ones we don't yet know about.

2.3 Worms

Often people refer to viruses and worms as the same things. However, there are two major distinctions: the ability to travel alone and the ability to stand alone as separate programs.

Viruses require human intervention to start replicating. That is NOT true of worms. A **worm** can make copies of itself on a network or move by itself using email without any human intervention.

Worm A standalone malware program that copies itself across networks.

A worm is also usually a standalone program. A worm *transmits itself* between machines across a network. A virus *attaches itself* to files. When a virus copies itself, it is copying itself to other files on the same machine. (A virus spreads to another machine when one of the infected files is moved to another machine, in most cases by a user who does not realize that her files have been infected.) A worm copies itself to another machine rather than another file on the same machine.

The end result of all that copying is usually denied service. Someone, somewhere who wants to use a network resource can't get to it because the worm is taking up so much disk space or bandwidth. Often, worms initiate a denial of service (DoS) attack against a specific website. Code Red targeted the White House website.

Other worms send out so much garbage data that substantial parts of the Internet stop responding. Financially, this can be devastating. When Slammer brought the

Net to its knees, Continental Airlines had to cancel flights from Newark, New Jersey, because it couldn't process tickets. Slammer also brought down emergency services. Outside Seattle, 911 dispatchers lost access to their call centers. While no deaths were directly reported from this outage, fate could easily have taken another turn.

Worm Number 1

In the early 1980s, Xerox researchers John Shoch and Jon Hupp designed an application to automate installing and updating software across a network. When that application hit a bug, it distributed the bug as well. Shoch and Hupp noted, "The embarrassing results were left for all to see: 100 dead machines scattered about the building." They had unwittingly created the first network worm.

Our society relies on computer networks for a lot more than banking and education. The Sasser outbreak was widely believed to have crashed a train radio network, leaving 300,000 train travelers stranded in Sydney, Australia. Of course, computer networks link more than just our transportation systems. They also link our hospitals and ambulances. Many traffic lights are also computer-controlled. It may only be a matter of time until those pranks prove deadly.

Worms have many ways of getting into your system without your knowledge. They can make their way into your computer from the Internet through a security flaw. You might run a cool game on your computer, but it is really a worm that tricked you into running it by making you think it was only a game. Sometimes, you don't need to do anything. Some of the more devastating worms, Code Red and Slammer, actually spread with NO action required by the user at all.

Worms are also designed to be *fast*. The speed at which they are released once a security flaw is found but before a patch is released is amazingly fast. To make matters worse, **script kiddies** start releasing variants.

Script kiddie A low-talent hacker (often an immature teen) who uses easy, well-known techniques to exploit Internet security vulnerabilities. In the hacker community, being called a script kiddie is a major insult.

One infamous script kiddie was Jeffrey Lee Parson. While still in high school, he released a variant on the Blaster worm. The real malware writer—the person who wrote the original Blaster worm—was never found. Parson was just a copycat. Like Parson, almost anyone can make minor alterations to code. It doesn't require the same skill or creativity that you would need to actually create a worm or virus. Still, the effects of minor alterations can be devastating. Mere weeks after Parson unleashed his Blaster variant, experts estimated that the worm had infected 500,000 computers worldwide. Even that wasn't all his own work. Parson's Blaster variant only infected 7,000 computers. After that, variants on his variant created by still other script kiddies took over.

As worms continue to become more complex and evolved, it isn't just the rate of variant creation that's speeding up. Infection speeds have also dramatically increased. During the Code Red attack in 2001, the number of machines infected doubled every 37 minutes. At the peak of the Slammer attack, the number doubled every 8.5 seconds!

2.3.1 Especially Wicked Worms

Like viruses, worms exist in many shapes and forms. These are some of the more notable worms.

Famous Worms

Worm Name	Release Date	Significance
Morris worm	1988	Robert Morris, Jr., a Cornell graduate student was responsible for what is generally considered to be the first worm released to the Internet. This worm affected 6,000 to 9,000 major Unix machines and shut down a good bit of the Internet as it existed at that time. Morris himself became the first worm writer arrested for his exploits.
Melissa	1999	Melissa was a blended threat that included a virus that attacked Microsoft Word documents. When users opened an infected document, Melissa accessed the user's email address book and mailed itself to up to 50 people.

continues

Famous Worms *continued*

Worm Name	Release Date	Significance
I Love You	2000	The I Love You worm arrived in the form of emails having the Subject: line "I love you" and carrying the attachment, Love-Letter-For-You.txt.vbs. Readers who opened that attachment had their PCs searched for passwords which were emailed back to a website in the Philippines. The worm then re-sent itself to every contact in the reader's Outlook Express address book. This worm makes the list for using social engineering to create a message that even readers who knew better simply HAD to read.
Code Red	2001	Code Red attacked websites rather than PCs. First, Code Red defaced infected sites with the message: `Hello! Welcome to http://www.worm.com! Hacked By Chinese!` At the trigger time, midnight July 19th, infected servers stopped infecting other servers and initiated a massive DoS attack against the White House website. This attack failed only because experts identified the target—on the 18th—and moved the White House website to a different Internet address.
Slammer	2003	Known as "the worm that crashed the Internet in 15 minutes." Slammer *literally* slammed into the Internet at full speed. Within 10 minutes, Slammer had infected 90% of its targets. Within 15 minutes, important parts of the Internet became unusable.
Sasser	2004	Unlike many other worms, Sasser was NOT a mass-mailer. Instead, it attacked via operating system security holes and spread without user intervention.
Conficker	2008	Conficker used a variety of malware techniques to take control of infected remote systems. First detected in November 2008, by January 2009 Conficker had gained control of between 9 and 15 million PCs in nearly 200 countries.
SillyFDC	2009	By late 2010, this worm had gained substantial ground compromising infected machines by downloading and installing additional security threats.

2.3.2 Variants and Mutations

While a single worm or virus is bad enough, few pieces of malware remain in their initial states for long. The original authors, as well as other malware writers, continuously produce new variations on old attacks. The MyTob worm gave rise to 12

additional mutations by month's end. Netsky, in its first six months in the wild, evolved into 29 variants.

Got a minute?

At top speed, Code Red infected over 2,000 servers a minute!

With a biological virus, a single tiny mutation in the virus can mean that the vaccine no longer works. With a computer virus, a tiny variation in the code can prevent antivirus software from identifying the virus. Virus writers know that once someone creates a new virus, they can simply add a few tweaks and get their **variant** past the antivirus engine. Some viruses are even polymorphic and can alter themselves.

Fortunately, antivirus software can detect many new variants through the use of heuristics. Still, variants and mutations continue to cause problems. This is why your antivirus software must be up-to-date. If your virus software hasn't been updated since last week, you don't have the new signatures. And last week's signatures might identify last week's viruses, but not this week's new viruses and mutations. Most mutations are changed just enough to render the last virus signature invalid.

Variant A mutated form of a virus or worm. Variants are usually just different enough that the original virus signature won't match.

To avoid getting slammed by last week's news, always make sure your antivirus software is configured to download updates *automatically* from your antivirus vendor. Don't forget—anti-virus software is only one piece of the security puzzle. Firewalls and intrusion detection/prevention systems can also detect various worms and can be used to prevent unwanted connections. Intrusion prevention software is often bundled into firewall software—software that allows you to detect and sometimes block known attacks from getting into your network.

2.4 Trojan Horses

The name "Trojan horse" derives from Greek mythology. In an exploit reported by the epic poet Virgil in the *Aeneid*, the Greeks gained entrance to the city of Troy by presenting the Trojans with a gift of a giant wooden horse. Delighted by

the gift, the Trojans took the horse beyond the gates and into the city. Overnight, scores of Greek soldiers who had hidden inside the wooden horse emerged. They slew the Trojans in their sleep and opened the gates of their city.

In computer terms, a Trojan horse has a similar objective: to camouflage itself as something harmless or desirable, then to open the door and let attackers in. Just as the ancients learned to "Beware of Greeks bearing gifts," you should always question the motives and real purposes behind free software.

The idea with any Trojan is that it needs to be enticing enough that users will want to run it. In reality, the real purpose of many Trojans is to open a "backdoor" to your computer that allows for easy re-entry. The backdoor allows someone else to control your computer system or access your files without your permission or knowledge. This allows the attacker to return later and steal your confidential information or even use your machine to attack someone else's.

The methods used to trick recipients into installing the Trojan vary. One underhanded approach in 2009 was the Swine Flu Trojan. In this attack, users received an email spoofed to make it look like it came from the Centers for Disease Control and Prevention. The emails, carrying Subject lines such as "Governmental registration program on the H1N1 vaccination" or "Your personal vaccination profile", directed users to create an online profile for their state's H1N1 vaccination program. Users who clicked the provided link installed a Trojan instead.

You can run a Trojan program without actually knowing that you are doing so. Undetected Trojans are lethal and when mixed with a **zero day** attack, they have the potential to cause mass destruction.

A zero day attack is an attack based on a security hole that the experts don't know about. Thus, there's no easy remedy to stop the attack. The Aurora attack was a zero day attack mixed with a Trojan that was used to siphon out confidential information. By the time McAfee Labs discovered the attack on January 14, 2010, the damage had already been done to Google and a reported 34 other companies.

Zero Day attack An attack that takes advantage of a security hole for which there is no current patch.

At first glance, that probably sounds strange. Aren't ALL attacks based on a security hole we don't know about? Surprisingly, no. Most attacks take advantage of fairly well-known vulnerabilities. Those attacks succeed mostly because users don't do a good job of applying updates and patches to fix those vulnerabilities.

Zero day attacks are problematic because there really isn't a good way to protect yourself from a problem that the experts don't know about yet. The Aurora attack is believed to have begun in late 2009, running undiscovered by most victims until mid-January 2010. The Aurora attack was incredibly sophisticated. It used a combination of malware programs, some of which used multiple layers of encryption to hide their activities. The attack was aimed at Google's mail system (Gmail) as well as dozens of other companies involved in technology, finance, media, chemicals, and defense. Because the Gmail attack targeted the accounts of Chinese dissidents, some pundits suggested potential Chinese government involvement.

While Aurora was used mostly to steal source code and other intellectual property from corporations, other Trojans are created specifically to collect information from teens and consumers. For example, Trojan Win32/PSW targets online gamers. This Trojan installs a keyboard logger that captures gamer logins. Thieves use those logins to steal gaming avatars, virtual cash, and treasures.

Sometimes, running a Trojan can also unleash a computer virus or a worm. This combination of nasty code operating together is called a **blended threat**. By attacking in several ways simultaneously, blended threats—even those that aren't zero day attacks—can spread rapidly and cause widespread damage.

Blended threat A form of malware that includes more than just one attack. A blended threat could include a virus, a worm, a Trojan horse, and a DoS attack all in one attack.

2.5 Bot Networks

The Zombie Machine

Tabitha, a junior at Gettysburg Area High School, got off the school bus and ran home to check her email. Because she has friends (real and virtual) spread around much of the world, this is something she did at least 3 times a day. No Internet. Three hours later, still no Internet. And no Internet still later that evening.

Assuming there was a problem with her service, Tabitha had her father brave the rounds of "Please hold" and recorded ads to actually talk to her cable company. What they learned was unexpected and pretty frightening. Earlier that day, her cable company had tracked hundreds of emails coming from her connection. Seeing the massive outflow of email, the cable company cut off her service. Unfortunately, they didn't tell her.

Tabitha was clueless. Like a growing number of home users, Tabitha's parents had networked their home. A simple router (under $50 at Staples) split her Internet cable allowing access from both her computer and her parent's machine. Apparently, her computer had been the victim of a BOT network attack that gotten past the router firewall. Someone else had taken control and was using her PC to launch attacks against other computers. The attacker had literally turned her computer into a "zombie".

This teenager's computer had become part of a bot network. A **bot** network is a collection of compromised machines often called zombies. Each **zombie** machine is under the command and control of the malware writer or hacker—almost always without the knowledge of the machine's rightful owner. The owner of the botnet can issue instructions from a central location, and all of the zombies will carry out these instructions, often to attack more hosts. Tabitha certainly had no idea that her PC had been enlisted in a bot army. Likewise, Tabitha had no idea who took over her machine. She didn't even know what website they were trying to attack. If her father hadn't called the cable company, she may never have even known that her PC had been hijacked. What she did know was that losing her own service, however temporarily, was incredibly frustrating. She also found the idea of having some stranger control her computer just plain creepy.

Zombie or Bot A computer that's been compromised by a piece of code that allows it to be controlled remotely without the computer owner's knowledge.

A **bot network** is a collection of computers that have been infected by a worm or Trojan which installs code (known as a bot) that allows the attacker to launch remote commands and use the systems for future attacks. The "bot" code opens a backdoor that allows the hacker to control the machine and initiate commands remotely.

Bot network A collection of remotely controlled bots. Hackers often use bot networks to launch attacks against other computers.

Once a hacker has assembled a bunch of machines compromised with bots, what he has is literally an army of "bots" that can be used to attack other machines. Frequently, the bots execute a denial of service (**DoS**) attack where so many compromised machines try to connect to a single website that the site itself crashes. In this type of attack, the goal is to flood the target machine with data packets. The data transmitted is usually harmless itself, but the large amount of traffic consumes the target machine's bandwidth. It uses up the Internet resources available to the target machine, keeping it from being able to communicate properly.

The end result is the same in all cases. Legitimate users are denied service because of all the bogus traffic.

DoS A denial of service attack. In a DoS attack, the victim is flooded with so much Internet traffic that legitimate users can't get through.

In recent years, bot networks have been used to attack some of the biggest names in the computing and corporate worlds. Because bot networks are assembled randomly across the World Wide Web, a single command can launch a DoS attack by bot networks at any time, from any place in the world. Or even many places in the world simultaneously. March 2009 saw the identification of a major bot network dubbed "Ghostnet" that included over 1,200 compromised machines in 103 countries.

The majority of machines compromised by bots are outside the United States. By mid-2009, the U.S. held only 18% of bot-controlled machines. Still, that's a huge number of compromised machines. From mid-2008 to 2009, the number of bot-infected machines jumped 50%. McAfee Avert Labs found 12 million new bots just in the first quarter of 2009.

If the threats have been growing, so have the attacks. In a single attack in June of 2004, a massive bot army of compromised home computers managed to shut down the websites of Apple Computer, Google, Microsoft and Yahoo! for a full two hours. How could a single attack kill the websites of four major computer firms at one time? In this case, by focusing on a fifth firm, Akamai. Akamai runs domain name servers that translate domain names, such as www.microsoft.com, into the numerical addresses used by the Internet. Basically, Akamai controls the address book that takes Internet users to certain websites. It so happened that Apple Computer, Google, Microsoft and Yahoo! were all Akamai clients.

So what can you do to keep your machine from attacking other computers? It would seem that the logical solution is to patch your machine. You need to make sure that you've applied all the current patches to your operating system and web browser. However, the real question is how to protect yourself from bad bots (i.e. zombie makers). The first step, as in almost all computer security issues, is to make sure that your antivirus software is installed correctly and ALWAYS up-to-date. It must include anti-spyware and anti-adware detection and removal capabilities. And you should make sure that your PC is sitting behind a very well-defined firewall.

2.6 Social Engineering

Nasty code has been around for over 20 years now. We all know that opening attachments is dangerous, and sharing files can leave you without valid files of your own. Still, every year millions of users fall victim to malware.

A common reason is the use of **social engineering**. Social engineering involves understanding human nature and using that understanding to take advantage of users. It allows malware writers to trick users into breaking their own security

rules. Sarah Granger, writing for *Security Focus*, put it well when she defined social engineering as, "a hacker's clever manipulation of the natural human tendency to trust."

Social engineering Using general knowledge of human behavior to trick users into breaking their own security rules.

A good example of the use of social engineering to spread malware was seen in the Love Bug attack. Most people who opened this virus did so for one of three reasons—all related to basic human psychology:

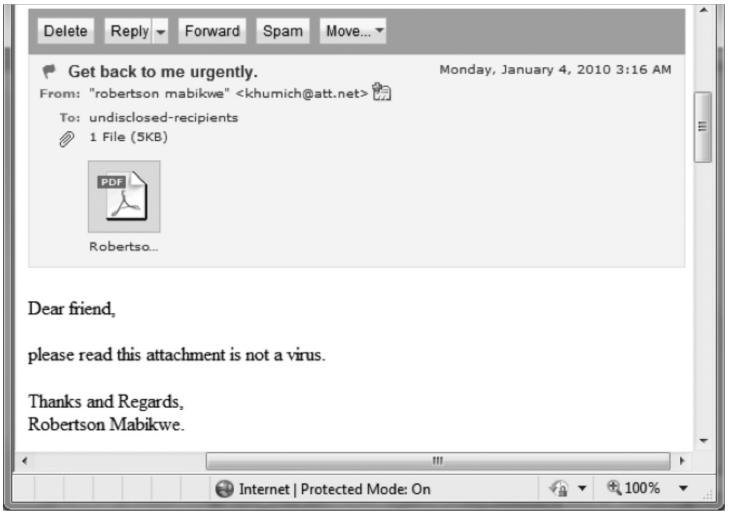
1. The email came from someone they knew and trusted—a colleague, a spouse, an old friend. Someone who might possibly really love them.
2. They thought the email was a joke. Millions of jokes (some much worse than others) circulate the Internet each day. For home users, these humorous anecdotes account for a good percentage of email usage.
3. They just couldn't help themselves. "I love you" messages from distant colleagues, regardless of how unlikely and bizarre, simply jolt the recipient's curiosity.

Of course, social engineering touches more than users' romantic lives. Some common uses of social engineering in malware include guessing passwords, spoofing emails to appear to come from acquaintances, masquerading as authority figures, and never underestimating the human capacity for greed.

Don't I know you?

People love keeping in touch with each other. Spammers rely on this, generating `Subject:` lines that trick the user into believing she might know the message sender. Love Bug relied heavily on this factor to entice users to open the attachment. How easy would it be to trick you into opening an infected PDF someone sent you?

Would you fall for this one?



This example, like many attacks in the last quarter of 2009, exploits a vulnerability in the Adobe Reader program that your computer needs to display PDFs. Like most attacks, this is not a zero day attack. The security hole being targeted was identified and patched some time ago. Yet, these type of attacks succeed because so many users haven't installed the newer versions of Adobe Reader or applied the security fixes.

2.7 Avoiding Malware

Avoiding malware is getting to be a lot more complicated than it used to be. In the past, users could protect themselves fairly well simply by not sharing documents and not opening email attachments from people they didn't know. Today, that's just not enough. Today's user needs to know what to do as well as what not to do.

The first step to protecting yourself from nasty code is to be proactive as well as reactive. Make sure you have the basics covered:

- Install a top-rated antivirus package. No excuses here about not being able to afford it. Microsoft Security Essentials provides free antivirus protection that helps protect your computer against viruses, spyware, and other malware. AVG and Symantec also have free antivirus software (Symantec if you are a Comcast user).

- Use the automatic update option on your antivirus software. Remember that new mutations appear continuously. Automatic updates will help to keep your virus signatures current.
- Be sure to install patches to ALL the software you use. That includes browsers, plug-ins (like Adobe Flash Player), and utility programs like Adobe Acrobat and Adobe Reader.
- Download software only from first-party websites. If you need a new version of Adobe Flash Player, go to the Adobe website. Don't click links in pop-up windows.
- Be very careful about any "free" downloads. Remember that malware often masquerades as freeware.
- Be wary of email from people you don't know. Never open attachments to emails of unknown origin.
- Also be wary of email from people you do know. Some attacks appear to come from someone you know. Also, many worms resend themselves to every person in a victim's online address book. Think long and hard before opening an attachment that you weren't expecting. Call or email the sender first, just to be sure.

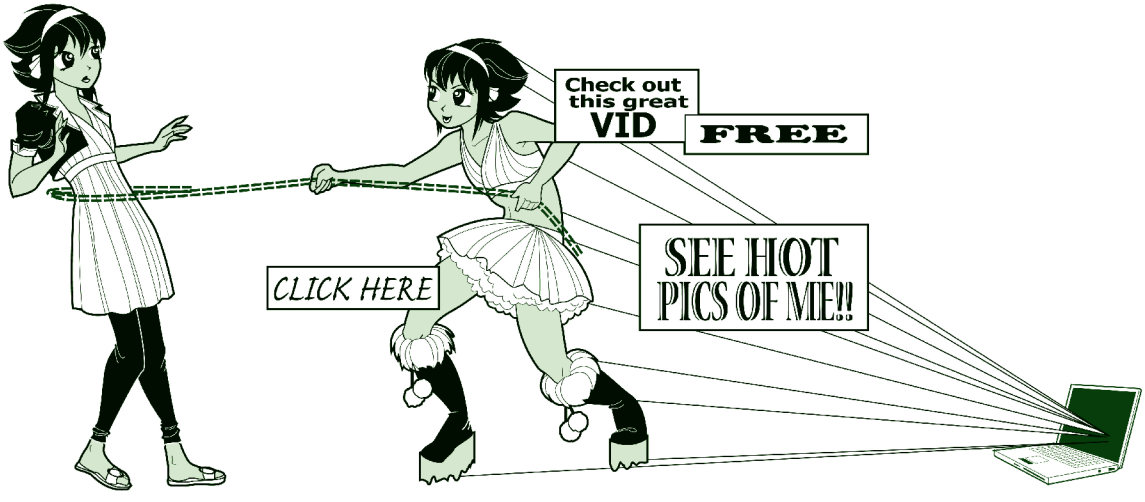
Chapter 3

Nasty "ware"

Meet Stef from Camden, Maine. Stef loves music and enjoys downloading the latest hits to her iPod.

When Stef received an email offering her ten free songs, she didn't hesitate to click the embedded link for more details. Now her PC is under siege from advertisers and continually plagued with pop-up ads.

Stef thought she was only getting a few songs. Little did she know that "free" doesn't always mean "free."



Stef had fallen victim to adware—one of a number of nasty "ware" problems out there. Like spyware, rogue security software, and ransomware, adware is a major problem for users. While Stef thought her antivirus software would protect her from problems like this, doing that's a lot harder than it sounds. Adware and spyware are really in a class of their own. McAfee refers to programs like these as potentially unwanted programs or **PUPs**. That's a bit generous, since most spyware is unwanted, and we've yet to meet anyone who *really* wanted adware. And while security software like antivirus products try to stop PUPs, or at least warn you about them, the adware writers are continually changing their software to avoid detection.

PUPs Potentially Unwanted Programs. A politically correct term for unwanted adware and spyware.

Still, those PUPs are being dumped on systems and some are collecting data about you. These **data grabbers** often collect information without your knowledge and send that information on to someone else or save it in a special file for pickup later (at the convenience of the hacker). Sometimes, a third party uses the information to target advertising. They're basically looking for better ways to sell you things. Other times, that information is used to steal your identity or take over your computer.

Data grabbers Software programs that collect information about you and send that data on to a third party. Data grabbers include adware, spyware, and keyboard loggers.

3.1 Spyware

Some companies sell legitimate "spyware" programs. Many forms of parental control programs in effect spy on users. So do employee monitoring programs. These are not what we mean when we talk about spyware. In this book, we cover malicious spyware. That is, programs installed without your knowledge that can eat up system resources, affect performance, and steal confidential information. As the name suggests, **spyware** literally spies on you when you use your computer. Among other things, it may keep track of which websites you visit and what you

do on those sites. Spyware may also include keyboard loggers which collect the user names and passwords that you enter at various sites.

Spyware A software program that monitors your computer usage without your knowledge.

Spyware is different from worms and viruses in that spyware's primary purpose is to spy on you. It doesn't self-replicate. Even so, spyware is just as dangerous. If you care about your privacy, you need to understand how spyware lands on your machine and whether you or your parents are at risk.

If your system has slowed down for no apparent reason, you may already have spyware because you visited a malicious or compromised website and the program installed without your knowledge. This type of code dumping is called a **drive-by download**. Some spyware will even install after you say No to installing it.

Drive-by download A program that is installed without your knowledge when you visit a malicious or compromised website.

3.2 Adware

Depending on who you ask, **adware** is either legal commercial software or it's malware that's dumped on a users' systems without their knowledge or truly informed consent. Some people refer to adware and spyware as the same thing, but they're not.

Adware is a type of software that delivers advertising to your Web browser. Advertisers also use adware for what they call behavioral targeting. It allows them to target ads to the consumers most likely to purchase a given product based on those consumers' other online activities. There actually are some legitimate uses for adware, and most adware manufacturers try to stay within the letter of the law by requiring users to consent to having their programs installed.

Adware A program that delivers targeted advertising content to users often by gathering information from a user's computer about what that person does online and which websites are visited.

Adware can be incredibly annoying. It can change your homepage, flood your screen with multiple pop-up ads, install tool bars in your Web browser, and read cookies installed on your computer. It can also arrive without your knowledge.

Teens who are heavy Internet users can easily get adware dumped on their PCs without realizing it. These programs can hitch a ride when you download free tools such as screen savers, or if you visit a malicious website. Teens also often download adware along with popular software, music, and video files.

While adware is usually unwanted, sometimes it's an "I'll scratch your back if you scratch mine," situation. In a common scenario, websites will allow you to download "free" software in exchange for taking adware as part of the package. Of course, that software really isn't free. You're *selling your time* in watching (closing, or trying to close) all the pop-ups in exchange for the software. This may not necessarily be a bad deal. Consider. If your cable company gave you free cable TV in exchange for using a system that stopped you from filtering out the commercials, you might still feel you were getting the better end of the bargain. That's pretty much the deal you're making when you use some popular file-sharing software. The trick is to realize the deal you're making.

3.2.1 End User Licensing Agreements (EULAs)

Many users don't realize that they've consented to install adware because they don't read the **End User Licensing Agreement (EULA)** when they install new software or sign up for new Internet services. This is understandable. EULAs are typically long, boring, and written in legalese. Often, they're presented in small type and confusing language, and most users wrongly assume they don't cover anything that's terribly important. Some companies provide EULAs that are written in such wordy, convoluted text that only the most determined geek will even attempt to decipher their meaning. The adware application TinkoPal provides a EULA that contains over 5,000 words artfully arranged into only 145 sentences of nearly 40 words each.

EULA End User Licensing Agreement. This is the detailed legalese document that you must agree to in order to install most programs.

While it's hard to get around deliberately misleading EULAs, truthfully, few companies bother because they assume you're not going to read the EULA anyway. Quite a few are very upfront and actually list the adware functions. This type of download leaves the adware company on legal ground, because they can argue that you said yes to installing it in the first place, even though you may feel that you were tricked.

3.2.2 Peer to Peer (P2P) Networks

Peer-to-Peer (P2P) networks are places where teens often visit to share resources such as music, films, software, games, and other programs. While it's gone seriously commercial now, Napster began as a popular P2P network. With P2P, you can search online and share files with other people who are using the same file sharing program. Common file-sharing programs include Kaaza, LimeWire, iMesh, and Bit Torrent.

Downloading items from P2P networks is very popular for a number of reasons. These are places to find content that's offbeat, new, or edgy. If you're looking for Indie retro techno-punk, you're probably going to find it on a P2P site. Downloads from P2P sites are also often free. And risky.

Why risky? Commercial sites tend to be extremely careful about what they allow to be downloaded. If they aren't, people are likely to sue them for downloads that trash their systems. Artists are likely to sue them for violating copyright laws. When money's involved, people are likely to sue in general. While those lawsuits (or just the fear of them) drive up the price, they also add incentive to site operators to ensure that their downloads are safe and legal.

Things get riskier when you start downloading from unknown sites and sites that rely on individual submissions such as P2P networks. Downloading games, movies, and music from unknown sites can get you into trouble on several levels. You might download malware, adware, spyware, Trojans, and keyboard loggers. You may also violate copyright laws and face fines for piracy. Even if the material you're downloading is safe, your download experience may be more than you expected. Specifically, you may have agreed to accept adware when you installed the software you need for P2P file sharing.

At this point you're probably thinking, but I really *need* to download free stuff! That's one of the reasons I wanted a PC to begin with. Don't despair. While you may or may not *need* to download free stuff, you certainly don't *need* to use an adware version of download software to do so. Many P2P services offer a commercial download package that's free of adware. The catch of course, is that it is commercial—meaning you'll need to pay for it. If the price tag makes you balk, remember that you ARE paying for the free downloads. You're selling your time (to watch ads) and details on your personal browsing habits. For many people, that price is simply too high.

3.2.3 Downloading Safely

There are many "things" you can download to your computer—a song, a film, a new screensaver, a game, another type of software program. But before you download anything ask yourself these questions:

1. Can the site you're downloading from be trusted?
2. Is the "thing" you're downloading a legal copy or do you think it's probably pirated? Are you breaking copyright laws?
3. Will adware get dumped on your computer? (Not sure? Carefully read the End User License Agreement!)
4. Is the file-sharing software you're using to download this item really free? Or, are you paying for it by selling your time to watch ads? If so, are you OK with that?
5. Is the "thing" you want to download safe? Could it contain malware like a Trojan? Are you willing to take that risk?

3.3 Keyboard Loggers

Keyboard loggers are integral parts of some adware and spyware programs. Other keyboard loggers are installed separately as standalone programs, and marketed as employee or parental monitoring systems.

A **keyboard logger** is exactly what it sounds like, a program that logs every keystroke that you type at your computer. This can be incredibly dangerous. Just think about some of the things that you type in. If you use online banking, you enter the user name and password for your bank account, maybe even the account numbers. If you order games or clothes online, you enter your parents' credit card numbers. If you apply for credit or jobs online, you enter your social security number and other personal data—everything a thief would need to take over your identity.

Keyboard logger A program that keeps track of every keystroke that you type at your computer.

Hackers have been planting keyboard loggers on users' PCs without their knowledge for many years. Short of outlawing keyboard loggers, which probably wouldn't help anyway, the only solution to this problem is to adequately protect your machine. Outlawing loggers isn't an option anyway. Keyboard loggers are a standard part of any security expert's tool bag. Experts use these tools in investigations to catch bad guys doing bad things.

As an interesting side note, some of these keyboard loggers are marketed to parents to monitor teen activity online! If you think you're immune, reconsider. A 2007 study by the Pew Internet & American Life Project found that 53% of parents with home Internet access use monitoring software. In addition, 45% use filtering software to completely block certain sites or types of material. Of course, sometimes it's the teens doing the monitoring. In mid-2008, a high school senior at an affluent California high school was arrested for installing software to track passwords on the school registrar's computer and then using the stolen passwords to change his grades.

3.4 Rogue Software and Scareware

In a cruel twist, some "spyware" exists only to sell anti-spyware solutions. These scams are referred to as **rogue security software** or **scareware**. Rogue software pretends to be legitimate security software. Some of these programs are quite

sophisticated and actually appear to BE your own security software informing you of a problem.

Rogue Security Software Also known as scareware. Applications that use unethical marketing practices to trick users into paying for and downloading worthless or malicious software masquerading as computer security software.

The most common rogue security software displays a bogus message announcing that your computer has been infected with spyware. The message is often formatted to display as if it were coming from your own security software.

The scammer then tries to sell you software to remove the "discovered" spyware. To add an air of legitimacy, most rogue security software uses a name that sounds trustworthy and familiar. The top sellers in 2009 were SpywareGuard 2008, AntiVirus 2009, SpywareSecure, and XP AntiVirus. Often, the same web page that generates the pop-up ad claiming your machine is infected actually *does* infect your computer with malware that continually redirects your web browser to ads for their software. Naïve users find that purchasing that software, for an average $49.95, just installs new and different spyware, and victims generally end up with a computer that's unusable.

This is an old game with a new face. In October 2004, the Federal Trade Commission filed charges against three companies, Seismic Entertainment Productions, Smartbot.Net, and Sanford Wallace, for what amounted to spyware extortion. The three firms first infected PCs with spyware that overwhelmed users with unwanted pop-up ads, then tried to sell them anti-spyware programs to fix the problems they'd just caused.

While the game is old, the tactics are new and evolving. Scareware ads now routinely appear where users don't expect them—like in the top page of search results from major search engines. How? Volume for one thing. By spring 2009, AVG's free LinkScanner tool, which helps prevent users from clicking on malicious Web links, was picking up 30,000 web pages a day that contained ads for scareware.

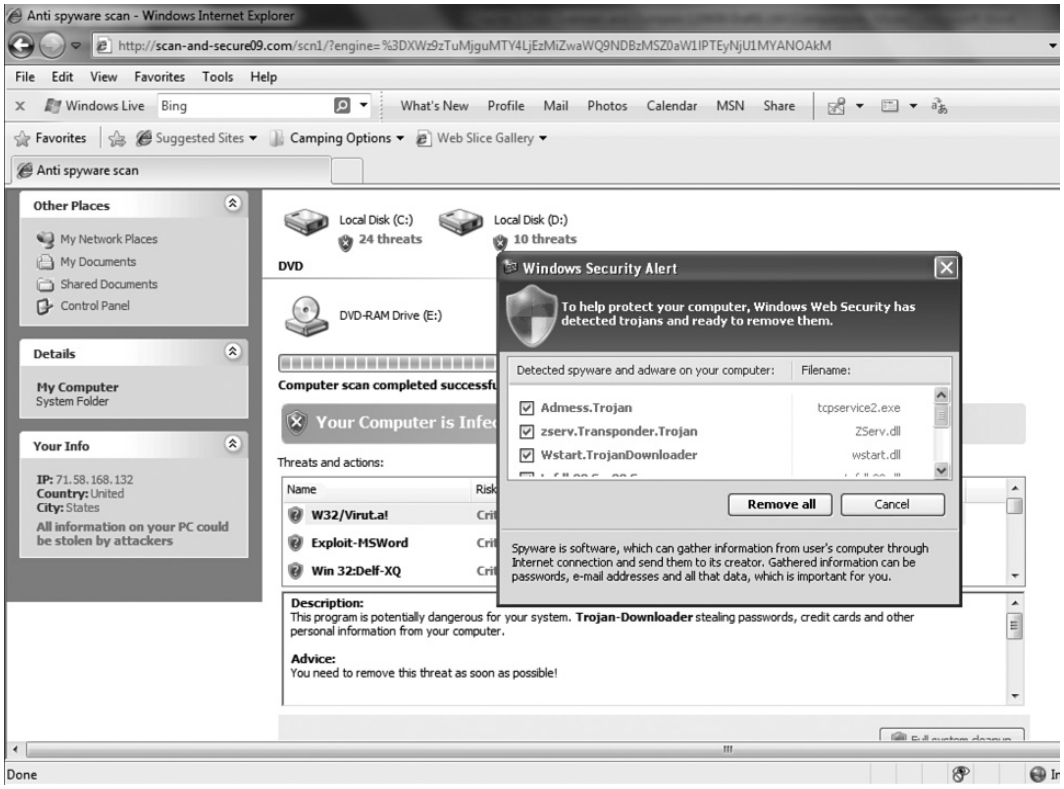
To increase hit rates, the scammers also include phrases that people are likely to search for often, like *American Idol* winner or NASCAR schedule. (We talk about this process, called black hat search engine optimization, later in this chapter.) Scammers also increasingly embed links on social networking sites, Twitter posts, and even within comments made on YouTube videos. In a practice known as **malvertising** (short for malicious advertising), ads for rogue security software have popped up on reputable sites (including Newsweek, Fox News, and the New York Times). The idea is to take advantage of users' trust of the reputable site.

Malvertising The practice of advertising rogue security software on reputable websites to exploit users' trust of those sites.

These scams are extremely common. Here is one we came upon while updating this book. At first glance, it looks legitimate doesn't it?

Our tip-off here was that our computer security software isn't named Personal Security and the people who wrote it understand enough English to write a better warning than "This computer is in danger with malware!" Truthfully, most rogue security software is more professionally written.

At the next level, they did do a better job at the scam. Notice how the next web page displayed looks like it isn't a web page at all unless you look at the address bar at the top. Instead, it's designed to look like a warning message from Windows.



Note that this is complete with the Windows logo on the pop-up identifying the alleged malware.

Regardless of what you click on this screen, you proceed to the download option.

Again, it doesn't much matter what you click here. Most scareware continues the download to infect your computer regardless of what you do at this point—**Run**, **Save**, or **Cancel**. If you're not running a good anti-malware program before you hit this point, you're in serious trouble.

This old game isn't likely to end soon. In April 2009, the *Wall Street Journal* reported that the number of scareware programs had tripled between July and December of 2008. By late 2008, the Anti-Phishing Working Group (APWG) identified over 9,000 separate scareware programs circulating on the Internet. In the first half of 2009, the APWG identified a **583%** increase in scareware programs. The scams appear nearly everywhere, including corrupted emails and even inside comments containing links on legitimate sites like YouTube and Twitter.

3.5 Ransomware

With **ransomware**, the creeps up the ante by holding your computer hostage until a ransom is paid. What distinguishes ransomware from general scareware or rogue security software is that the malware writers disable or threaten to disable your computer unless you pay up. Sometimes, that's an empty threat but one that it's fairly hard for the user to assess.

The most common form of ransomware is an extension of rogue security software. In this scenario, the malware you inadvertently install in response to the bogus spyware or virus report actually disables your files or critical programs until you purchase whatever software it is that they're trying to sell. Sometimes, however, the scammers give up the pretense of selling a product and are just upfront about the extortion.

Ransomware A form of malware in which the user's computer files are encrypted or the system (or Internet connected cell device) is disabled if a ransom isn't paid.

Ransomware is a form of malware that often targets mobile devices. Often, the "ransom" consists of sending a premium ($$$) SMS (text) message. One recent infection, Trj/SMSlock.A, demanded that infected users send a premium text message and include a supposedly unique number in order to receive the deactivation code. Thankfully, the code writers weren't very bright and security experts were able to release a free tool that generated deactivation codes. And by not very bright, we mean really, *really* not very bright, given that they displayed their ransom demands and instructions only По-русски (in Russian).

Most ransomware writers are brighter, albeit just as sleazy. One piece of malware spread in May 2009 through infected links in Twitter posts shut down and disabled all other software applications until victims purchased a two-year license of a rogue security software package for $49.95.

The crooks also don't always lock down your whole machine—just the files you're most likely to use. The LoroBot ransomware, identified in October 2009, encrypted all of the victim's text files, Word documents, PDFs, and JPG picture files, then demanded $100 for the decryption software.

3.6 Black Hat Search Engine Optimization

If you search online often, you know that even the most carefully worded search can return hundreds or thousands of results. While that seems great for all the websites returned, in practice, you know you're not going to look at more than the first few pages of any search result. In fact, odds are pretty high that you won't look at anything after the first 20 sites listed. Companies know this, and put a lot

of work into making sure that their websites appear within those first twenty sites returned. That process of ensuring that a website is returned as high as possible within a search result is called search engine optimization (SEO).

How does this work? The ranking assigned to any search result depends on a lot of factors. While most people assume that the top result is simply the most popular site, that's not the only factor considered. Google claims to use over 200 different factors when ranking websites. Although Google keeps their factors secret to attempt to foil spammers, most of the techniques used by the major search engines are well known. The popularity of a site, the content, the number of sites that have links pointing to it, and other factors are all used in search engine algorithms to determine a site's ranking. SEO uses these known factors to improve a website's ranking.

That ranking is very important. The higher a website is in search engine results, the more people will find the site. Most website operators want their sites listed on the first page of search results—the higher up, the better.

So, how does a website get a higher ranking? Well, content is the primary factor. The better the content, the higher number of links pointing to it. But quality of content is not the only factor. In fact, a website with quality content may not see a lot of new visitors with lower search engine results. No one will find the site. Enter the consultants, specifically, the Search Engine Optimization (SEO) consultants. Optimization is a fancy way of saying that a website will use the search engine algorithms to its advantage to gain a higher search engine ranking. SEO techniques and consultants modify the content and other data on websites and web pages to boost a website's ranking. Most of the major search engine operators even publish information for webmasters on how to structure their websites to do well.

By itself, SEO is a perfectly legitimate business practice. Where it becomes problematic is when it's used in sleazy ways. Have you ever done a search and gotten results that had NOTHING to do with what you searched for? Have you noticed returns for what looks like rogue security software when you searched for something completely unrelated to security? Well, some SEO techniques manipulate search engine algorithms using deception and illegitimate and unapproved means. These techniques are called **black hat SEO**. Some of the deceptive techniques include

stealing legitimate content from a popular website and posting it on a SPAM site, offering legitimate looking content to the search engine for ranking but providing SPAM sites to normal web surfers, and filling a web page with repeated words to increase the keyword counts for the search engine. The major search engines don't approve of these techniques and have modified their algorithms to lower the ranking on websites that attempt these techniques. That is, when they find them.

Black hat SEO The practice of using deception to give a website a higher search engine ranking than it deserves. Often used to direct unsuspecting searchers to pages filled with malware (like rogue security software).

Besides SPAM, black hat SEO techniques have been used for even more dangerous purposes. The main reason that SEO techniques are used is to increase the number of web browsers visiting a specific site. If a hacker wants you to try out his latest piece of malicious software, what better way to get interest in it? If he creates a website and uses black hat SEO techniques to get more people to find it, he'll have a large number of people to test it out for him. For the hacker, little effort is really needed to raise search engine rankings for his site.

Depending on his choice of keywords, the hacker can even pick a specific group of people to target. Kids are more likely to search for keywords like "algebra homework help" or "jonas brothers" than "retirement" or "dentures." Using black hat SEO allows a scam artist to route a teen searching for a particular gaming site to a fake gaming site that actually downloads malware instead of games. Always be careful when looking through search results. Just because a site is returned at the top of the list doesn't mean the site is necessarily relevant or safe. If the search engines can be fooled, so can you.

3.7 Current and Future Threats

The battle between users and hackers is a classic arms race. Both sides strive to stay one step ahead of the other. Recently, that struggle has become much more complicated for users. In the past, we only needed to worry about our home computers, and we could usually protect those fairly well with a standard antivirus software package.

Times have changed. Today's users spend more time online and on the go. Our computers now fit in our pockets and connect us with everyone, everywhere, at any time. We connect with our peers not just through email, but with tweets, texting, and real-time updates on Facebook and MySpace.

We expect—and get—instantaneous communication. Standing in line at a movie? We pull up reviews on our iPhones, check for tweets from friends who watched the film earlier.

While we're reaching out to the world, hackers take advantage of our connectedness and our willingness to trust. They find vulnerabilities in our smart phones, trick us into installing malware, corrupt search engine results, put up fake websites that look like the real thing, and use our constantly connected computers in botnets that deliver SPAM, attack other computers, and attempt to alter search results.

And the arms race continues. Hackers are constantly challenged to find new vulnerabilities, bypass security software, and trick users. Users must be constantly vigilant by installing and updating legitimate security software, updating that software as vulnerabilities are discovered, and avoiding the minefield of phishing scams, rogue software attacks, and fraudulent websites that deposit malware.

What does the future hold? For hackers, obviously more of the same. Hackers will continue to exploit any weakness they can find to get access to our personal computers, our private accounts, and our personal information. It is also likely that they will spread their efforts more widely, and we'll see more attacks on mobile devices. In many ways, our mobile devices are a more inviting target. They contain more personal information, are always connected, and have fewer methods for protection from attack. For users, the future holds greater responsibility and education. Understanding the importance of information security, particularly the security of personal information, will become paramount. And savvy users, like you, will make it a point to learn how and why to protect their data from hackers.

Chapter 4

Hackers and Crackers

Adrian Lamo started early. He dates his first "hack" (an especially clever computer use) to grade school—a tricky technique to double-write an old disk on the computer he had when he was 8. (Double-writing was a neat trick that allowed users to store twice as much information.) By 18, Adrian was on his own and making quite a name in the hacker community.

Adrian's specialty was breaking into the computer networks of top American companies. Dubbed the "helpful hacker" by the media, Adrian didn't take advantage of these break-ins. Instead, he reported his exploits to the network administrators of his victims and often the press.

By 2001, when he was still only 20, Adrian told a *Security Focus* reporter that his major problem was, "I'm running out of major U.S. corporations." Sadly, that really wasn't his only problem.

When the *New York Times* fell victim to Adrian's skill, they didn't say, "Thanks!" They pressed charges. Eventually, Adrian was sentenced to 2 years probation and ordered to pay restitution of over $64,000. Having faced up to 5 years behind bars, he got off easy.

Like Adrian, many hackers don't really expect to be prosecuted. Others just don't expect to be caught. The types and intentions of hackers have been changing. In the past, hackers defaced Websites simply because it was considered "cool." Today, hackers are financially and even politically motivated. In this chapter, you'll learn about the types of hackers and the tools that hackers use. We'll also discuss how you can learn more about security issues and careers in computer security.

4.1 Hackers

Many teens put their computer skills to use in hacking games—prowling the Internet for shortcuts and ways to "cheat" their favorite computer games.

While people use the same term, *hacking* computers is MUCH different than *hacking* games. Hacking a game by using a cheat is something many gamers do. Hacking a computer without authorization of the owner is a crime. Don't think it's cool simply because Hollywood puts a glamorous spin on it. Consider Jeffrey Lee Parson, an 18-year-old Minnesota teen arrested for releasing a variation on the Blaster worm. While Parson's goal was to make a name for himself as a programmer, what he got was a criminal record and 18 months in prison. Juju Jiang of Queens, New York was sentenced to 27 months for installing keyboard loggers at a Kinko's copy center and using the passwords logged to access victim's bank accounts. The convictions continue, and the sentences are becoming more serious. Brian Salcedo was a teenager when he broke into Lowe's computers and installed software to steal customers' credit card numbers, but he still got 9 years.

While early hackers (particularly teens), got off relatively easy, that trend is turning as the public becomes more aware of the actual costs of computer crime. Lawmakers have also tightened up statutes to include computer crimes. As one prosecutor, U.S. Attorney John McKay said, "Let there be no mistake about it, cyber-hacking is a crime."

4.1.1 What Is A Hacker?

In general usage, a **hacker** is someone who breaks into someone else's computer system or personal files without permission.

Hacker A programmer who breaks into someone else's computer system or data without permission.

Some experts like to use the term cracker instead, like a safe cracker, because hacker can also have other meanings. A small number of programmers like to call themselves hackers and claim that hacking is just coming up with especially clever programming techniques. There's some truth to this, but once Hollywood got hold of the term hacker, they didn't let go.

So long as the general public thinks of hackers as computer vandals and criminals, there's not much use trying to redefine the word. For this reason, when we talk about people who break into computer systems in this book, we'll be calling them hackers and not crackers.

In the early years, most hackers were computer geeks—usually computer science students—and often fit the profile of brilliant loners seeking to make a name for themselves. But don't forget that not all hackers have talent. Script kiddies are low-talent hackers (often immature teens) who use easy well-known techniques to exploit Internet security vulnerabilities. Hackers come from all walks of life. Some hackers are still computer science students. Others are former employees trying to get even with a company they feel wronged them. Still others are part of organized crime rings.

A current fear among law enforcement agencies is the emergence of **cyber-terrorists**. In our post-9/11 world, governments are beginning to realize just how much damage could be done to world economies if one or more outlaw groups were to fly the technological equivalent of a jet plane into the information highway. This was a major fear in the initial hours of the Code Red outbreak which targeted the official White House website. In theory, a cyber-terrorist could cause substantial damage by shutting down the world economy (literally crashing the computers that run the world's financial markets), or—more likely—by attacking infrastructure by attacking the computers that run our heating systems, power plants, hospitals, water purification systems, etc. When you consider just how technologically dependent most first-world nations are, the possibilities for disaster become nearly endless.

Cyber-terrorist A hacker or malware writer who uses a virus, worm, or coordinated computer attack to commit an act of terrorism against a political adversary.

While the Internet has yet to fend off a major terrorist attack, the potential for damage is staggering. Both the U.S. Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) recognize this threat. Currently, FEMA and DHS have teamed up in the Cyberterrorism Defense Initiative (CDI), providing free counterterrorism training to those people who provide and protect our national infrastructure. Classes are free to qualified personnel in government, law enforcement, firefighting, public utilities, public safety and health, emergency medical services, and colleges and universities. Clearly, cyber terrorism will remain a serious threat for the foreseeable future.

4.1.2 Black Hats, White Hats, and Gray Hats

When it comes to security, there are good guys, bad guys, and another set of guys who live halfway in between. These are usually called black hats, white hats, and gray hats, respectively. Since there are an awful lot of shades of gray, it's not always as easy as you'd think to tell the difference.

White hats

"White hats" is the name used for security experts. While they often use the same tools and techniques as the black hats, they do so in order to foil the bad guys. That is, they use those tools for ethical hacking and computer forensics. **Ethical hacking** is the process of using security tools to test and improve security (rather than to break it!). **Computer forensics** is the process of collecting evidence needed to identify and convict computer criminals.

Black hats

Obviously, the "black hats" are the bad guys. These are the people who create and send viruses and worms, break into computer systems, steal data, shut down networks, and basically commit electronic crimes. We talk about black hats at several points in this book. Black hats and malware writers are not considered the same thing in the security community—even though they are both breaking the law.

Ethical hacking Using security tools to find security holes and to test and improve security.

Some white hats work for computer security firms. This includes firms that defend companies from computer attacks as well as companies that help victims of computer crime to successfully prosecute the perpetrators. One such company, American Data Recovery (ADR), even provides an expert witness program. Computer Evidence, Ltd., takes an international approach to cybercrime, having offices in Europe, the U.S., Asia, South America, and the Middle East. Given the rise in computer crimes, **computer forensics** has become a quickly growing career option for serious programmers. Other white hats are specialty programmers employed by major companies and organizations. The job of those white hats is to close up security holes to protect their employers from the black hats.

Computer forensics The process of collecting digital evidence needed to identify and convict computer criminals.

Gray hats

Gray hats sit in the middle of the fence because sometimes they cross that ethical line (or more often, define it differently). For example, gray hats will break into a company's computer system just to wander around and see what's there. They think that simply because they don't damage any data, they're not committing a crime. Then they go and apply for jobs as security consultants for large corporations. They justify their earlier break-in's as some sort of computer security training. Many really believe that they're providing a public service by letting companies know that their computers are at risk.

Hats for All!

Want a view of all the hats in one room? Try DEFCON. Each July, hackers of all stripes and sizes make their way to Las Vegas for the meeting that bills itself as "the largest underground hacking event in the world."

Even teens who can pony up the registration fee are welcome to the event that *PC World* dubbed "School for Hackers"—an extravaganza of hacking tips, hacker news, book signings, and more. Of course, the good guys also show up. So often that "Spot the FED" has become a popular conference game!

The problem is that no matter how you look at it, a break-in is still a break-in. How would you feel if some neighborhood kids broke into your home and went through all your things just to show you that your house wasn't secure? Wouldn't you feel violated, even if they didn't break or steal anything? More importantly, would you hire those same kids to watch your house? Or, would you assume they were a little short in the ethics department?

4.2 Hackers Want Your PC

You might be thinking that hackers don't care about your computer, but they do. Hackers want access to your system for many different reasons. In ***Chapter 2, Know Your Villains***, we talked about "bot" networks and armies of "bot" networks. Once your system is compromised and connected into one of these armies, some hackers sell your system's name on a list of compromised PCs. Remember, once a hacker breaks in and plants a Trojan, the door is open for *anyone* to return. The hackers know this and are making money off of it. They know it's easy to hide and very difficult to track them back once they own your PC.

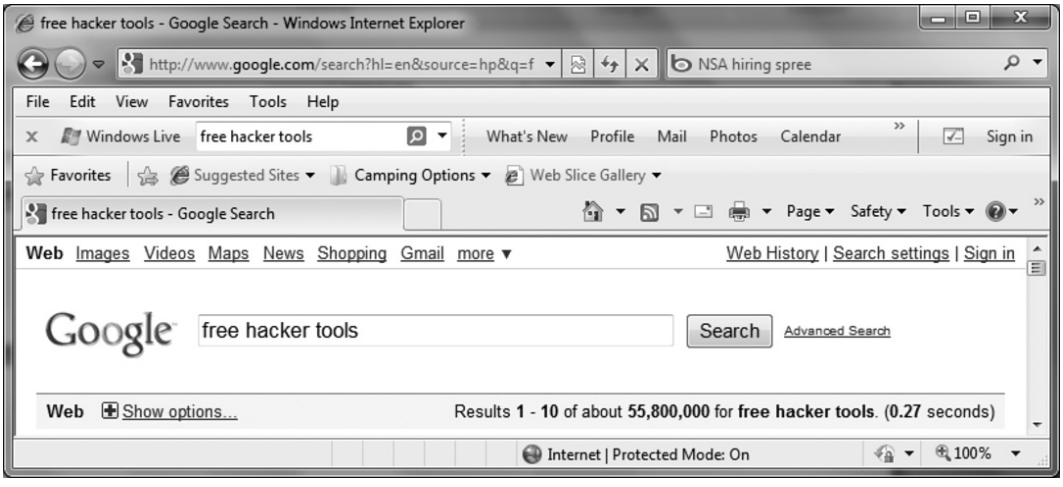
Overall, the Internet is an easy place to hide. Compromised computers around the world have helped to make hiding simple. It is easy to find the last **IP address** from where an attack was launched, but hackers hop from many unsecured systems to hide their location before they launch attacks.

IP address A unique address that identifies where a computer is connected to the Internet. Every computer, even yours if you're using broadband access, has an Internet protocol (IP) address.

Over the past four years, most cyber attacks have been launched from computers within the United States. However, this doesn't mean that systems in the United States are the original source of the attack. A hacker in Russia could actually use your computer to launch a denial of service (DoS) attack. To all the world, it might even look as if you started the attack because the hacker has hidden his tracks so that only the last "hop" can be traced.

4.3 Hacker Tools

In the old days, hackers would pass around tools in the underground. Today, hackers offer free tools all over the Internet. For an eyeful, try asking Google to search for "free hacker tools."



Granted, all 55 million+ hits aren't necessarily to the actual tools, but more than enough of them are to spread some serious mischief. The number also continues to grow. When we first published this book in 2007, this same search turned up only 20 million free hacker tool results.

Learning about these tools is important, but so is the way that you learn. Trying them out in a supervised lab or computer class is fine, but don't be tempted to test them out on the Internet on your own. Remember, hacking into a computer is against the law.

It can also be dangerous. Before taking a hacker tool from the Internet, ask yourself, "Can I trust hacker tools?" Really think about it. It could be a tool that really allows you to open a backdoor into someone else's system. Or, it could be a tool that conveniently opens a backdoor into *your* system. Maybe even both. And if it does compromise your system instead of someone else's, who exactly would you complain to?

4.3.1 Scanning Tools

Scanning tools are used by white hats to test system security. A good scanning tool will scan an Internet-connected computer for a wide range of security vulnerabilities. It might use "port knocking" to see whether your computer's Internet connection points are well guarded. It will also check which operating system you're running and look to see whether you've applied patches to the known security holes in that system. And, of course, it will give your firewall a workout, testing that your machine is protected from a wide variety of outside attacks.

White hats aren't the only people who can make use of scanning tools. To scan your own system, try Shields UP, a free scanning tool available from Gibson Research Company at www.grc.com. Also have a look at the many other scanning tools that GRC provides.

4.3.2 Password Cracking

Password crackers are among the most common and elementary tools in the hacker toolkit. These have been around for some time and are fairly effective at "guessing" most users' passwords, at least in part because most users do a very poor job of selecting secure passwords.

Forgot Your Password?

Join the club. So have 8 out of 10 computer users!

The first step to password cracking is often simple guesswork. This is made easy by social engineering. Hackers know that most users select simple passwords that are easy to remember. The top choices are nearly always names that are personally meaningful to the user—first names of immediate family members lead the list, followed by pet's names and favorite sporting teams. Password crackers may end up loading full English (and often Spanish) dictionaries, but they can hit a fair number of passwords with the contents of any popular baby name book. Other poor password selections include common numbers and numbers that follow a common format such as phone numbers and social security numbers.

Compounding the problem, many users set the same user name and password for all accounts, allowing hackers to have a field day with a single harvested password.

That's something to consider before you use the same password for Facebook as you use at school or at work.

Many users also make NO effort whatsoever to create useful passwords. In December 2009, the website RockYou was attacked and the passwords of 32 million account holders exposed. In the attack aftermath, data security firm Imperva analyzed those passwords. As is the case with most accounts that don't ban it, the word "password" was one of the most popular passwords. Also not surprisingly, a good number of users set the password for the RockYou site to "rockyou". Still, it was the numeric passwords that were especially lame. Half of the top 10 passwords were created by users who were either huge fans of Sesame Street's Count or insanely proud of having learned to count themselves. Those passwords? 12345, 123456, 1234567, 12345678, and 123456789. Other users in the top 10 apparently had prior experience with sites requiring numbers and letters. They set their password to "123abc" or "abc123". We've mentioned before that many computer criminals aren't all that bright. With passwords like this, they don't need to be.

The key to creating a *good password* is to create something that someone cannot guess or easily crack. Using your pet's name therefore is *not* a good technique. Using your login name is also a bad technique because someone who knows your login (or your name, since many login names are simply variations on your surname), could easily break into your system.

You also want a password that isn't easily cracked by the hacker tools. Automated password cracking tools have been around for decades now. These tools look for common names, words, and combined words. Therefore, one of the best methods is to use non-words with special characters to create a password. Many applications require seven or eight characters. To create an ideal password, make sure it contains at least 7 characters, use both numbers and letters, throw in at least one capital letter (since most passwords are case-sensitive), and include a special symbol like *, $, or #. For the letter portion, you can combine words that mean something to you but would be difficult to crack. For example, Linda's house is number 18, her pet's name is Flash, and she loves to look at the stars at night. So a good password for her to remember (but a hard one for hackers to crack) would be Flash18*. Don't be lazy and get stuck in the habit of using weak passwords.

Another important rule is NOT to use the same password for multiple accounts. For heavy computer users, this is a hard rule to follow.

Good passwords These are non-words created by combining things you can remember, such as your pet's name, your street address, and a symbol.

Since the major problem with setting passwords is users' inability to remember secure passwords, it is unlikely that this problem will abate until passwords are replaced with easier forms of technology such as **biometrics**. Biometrics is the use of secure biological data for identification. Common biometric systems use fingerprints, voice recognition, and retinal (eye) scans. The great advantage to these systems is that users can't forget them, it's nearly impossible to accidentally (or deliberately) pass them onto another person, and they're incredibly difficult to fake.

Biometrics The use of biological data, like fingerprints or retinal scans, for identification.

4.3.3 Rootkit

The ultimate goal for a hacker is to own total control of your system without your knowledge. A **rootkit** is a type of malicious code that can make that happen. Specifically, a rootkit is a collection of tools that a hacker uses to do two things:

1. Gain full access to a compromised computer or computer network
2. Hide the fact that the machine or network has been compromised

The first rootkits were created in the early 1990s. Since then, they've become very sophisticated. Today's rootkits open new backdoors for further access, collect user names and passwords, install and monitor keyboard loggers, and even attack other machines or networks. Rootkits even alter log files (to hide the fact that they've been compromised) and disable security software. Using these tools, rootkits can run in a way that they are fully trusted. They can hide from other software running on the system. And, they can escape detection by the programs used to monitor system behavior.

Rootkit A collection of tools that allows a hacker to gain full access to a vulnerable computer and hide his or her tracks.

So how does a rootkit arrive? The most common route is through an open security hole (like an unpatched operating system vulnerability) that allows the hacker to break into the target machine in the first place. Rootkits can also arrive via worms.

Some pretty serious computer attacks have been accomplished using rootkits. At one point, officials at the University of Connecticut had to admit that they'd discovered a rootkit that had been installed—and run undetected—on one of their **servers** for a year. The "rooted" server had contained personal information on a large number of students, staff, and faculty. While there was no evidence that the intrusion had resulted in specific thefts of identity, this left the University in the unenviable position of notifying 72,000 people that their names, social security numbers, birth dates, and telephone numbers *might* have been stolen. As Mark Russinovich, co-founder of the security tools site www.Sysinternals.com, told *eWeek*, "My guess is that there have been other discoveries in other places but we just haven't heard about this."

Server A computer that "serves" other systems by providing high-speed access to specific types of data, like personal files or email accounts.

No doubt other servers have been hit just as hard, as have home computers. Root kits are a type of malware that many Internet security packages don't routinely check for. Luckily, there are easily accessible free tools that will do so. Sysinternals, which was acquired by Microsoft in 2006, still operates a website that provides a variety of free security tools, including a RootkitRevealer. In fact, the entire set of Russinovich's Sysinternals tools—including RootkitRevealer—have been combined into the Microsoft Sysinternals Suite available for free download from the Microsoft TechNet page (http://technet.microsoft.com/en-us/sysinternals/).

Rootkit WOWs Startled User

While rootkits are often used for financial identity theft, sometimes the thievery is virtual. Consider this actual entry from the World of Warcraft forum:

```
0. Keylogger and Rootkit.TDSS help   12/16/2009 07:20:15 AM PST

My story goes like this. I let my WoW subscription freeze on November 16th 2009, and
on December 13th 2009 I decided to come back and renew it. However, when I checked my
account status it had already been renewed that very morning with an unknown credit
```

card. I logged into the game and found that my 80 warrior had been server transferred and stripped of all his gear. I got subsequently banned because the hacker had participated in illegal activity using my account.

I eventually changed my password, ran a few antivirus, and removed whatever malware I could find. I got the ban lifted, and started playing again yesterday. I tried to log in this morning and found that the password had been changed and my characters tampered with again. I've changed my password again using a different computer than the one I play on.

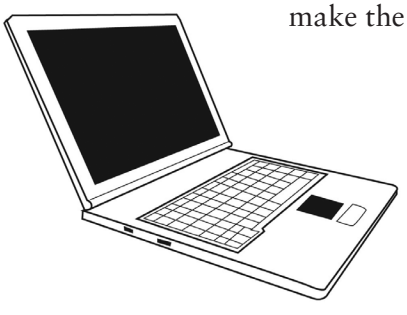
I suspect that I didn't catch the keylogger the first time around. I ran a few more scans with different programs and found that I have a Rootkit.TDSS infection and Trojan.Agent infection....

4.4 Calling White Hats!

With recent increases in computer crimes, and the decisions by law enforcement to treat computer crimes more seriously, there's come a growing shortage of white hats. Since supply and demand determine price, salaries are on the rise as well. According to a 2008 SANS Institute survey, over 98% of computer security professionals earn over $40,000 a year. A full 38% earn over $100,000 a year.

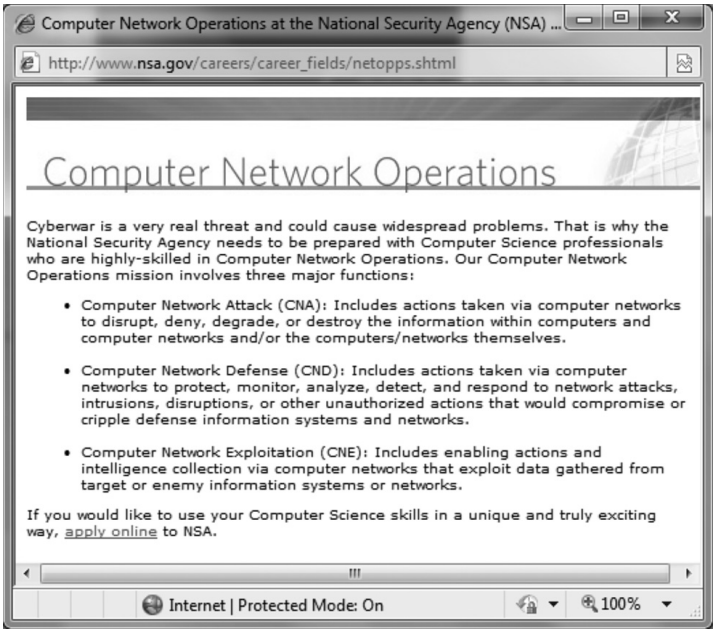
Even better is the outlook for employment. Even heading into the Great Recession in late 2008, as companies across the country began layoffs, 79% made plans to spare computer security personnel. The war on terror has also increased government need for security experts. In September 2009, Janet Napolitano, Secretary of the Department of Homeland Security, announced that DHS would hire 1,000 cybersecurity professionals by 2012.

There's a lot to say for being a white hat. In addition to great employment options and salaries, there's the bonus of knowing that you're helping to make the Internet a better and safer place.



If you're considering a career in computer security, look for colleges and universities that offer computer security as part of the computer science curriculum. Purdue University in Indiana, in particular, has had some famous white hats graduate from

its program. But they're hardly the only option. If funding's an issue (and truthfully, when isn't it?!), you might also consider looking into the scholarships offered by the National Security Agency (NSA).



To learn more about careers in computer security, ethical hacking, and security tools, have a look at some of these security sites:

- **http://securityfocus.com/** **SecurityFocus** is an independent site, not affiliated with any specific security product, that provides extensive up-to-date information about computer security to meet the needs of computer users and information technology professionals.
- **http://searchsecurity.techtarget.com/** **SearchSecurity.com** is a full-service site aimed at computer security professionals. This site provides a security-specific search engine, daily security news, sign-up options for security-related email newsletters, and over a thousand links to other security sites.

- **http://www.sans.org/** **SANS.org** is the official site of the SANS (SysAdmin, Audit, Network, Security) Institute, a world leader in computer security training. SANS provides many free resources, including weekly digests of security risks (@RISK) and general security news (NewsBites), as well as over 1,000 technical papers on computer security.
- **http://www.cerias.purdue.edu/** **CERIAS** is the Center for Education and Research in Information Assurance and Security. The CERIAS website provides a wide range of information related to computer security issues.

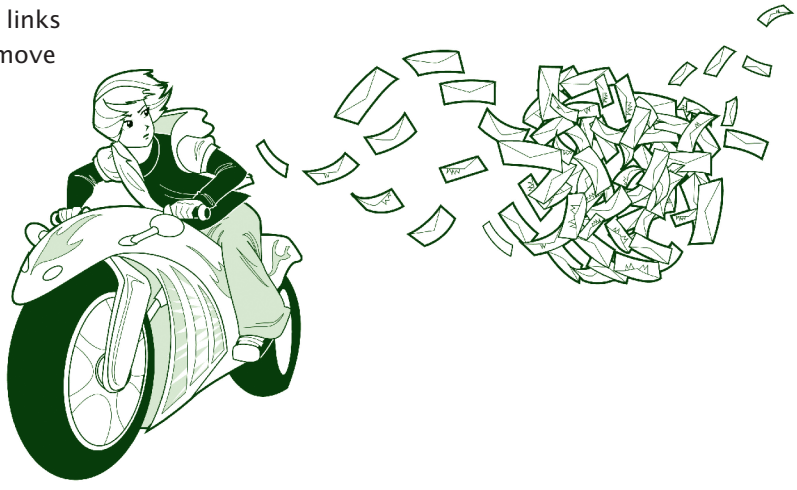
Chapter 5

Taking SPAM Off the Menu

Tessa was thrilled beyond expression on Easter holidays when her Dad finally relented and let her open her own email account. She checked it 4 and 5 times a day—eager to have mail of her own. Everyday it seemed she was giving her new address to someone else—friends at school, kids from her church youth group, even new friends she'd met online. To make sure that everyone could find her, she added her name to online directories and even posted her new address on her family's webpage.

The first month or so, everything was wonderful. Tessa felt connected to the world. Then she started to hear from some of its darker inhabitants.

First, Tessa began getting boring stupid emails intended for grownups. Silly people trying to sell her stuff no real 13-year-old could possibly want. Some of them even tried to get her to sign up for credit cards. Tessa tried to get rid of the emails, sending replies to links that were supposed to remove her from the mailing lists. The number of emails just kept increasing.



After a while, the mail Tessa was getting got creepy. She didn't really understand a lot of the things people were trying to sell her, but they reminded her

a lot of that day in Health class she always tried to stay home. And again, the number of emails kept rising.

By the last week of school, Tessa was getting so much junk email that she couldn't find the messages from her friends in the pile. She gave up and quit using her email.

As summer started, Tessa's dad signed her up for a new email account. This time, he defined filters to automatically throw away the messages she wouldn't want. Now, Tessa's being very careful who she gives her new email address to.

Like Tessa, most teens are overwhelmed by email they don't want and really shouldn't have to see. The sheer number of unsolicited email messages also wastes incredible amounts of computer resources. In 2009, a Microsoft security report concluded that 97% of all email messages are SPAM. How is that even possible? Thankfully, not all of that SPAM manages to get through. For every SPAM email you pitch, your Internet Service Provider (ISP) has blocked several more before they even land in your mailbox. Unfortunately, that still leaves a ton of SPAM in circulation.

5.1 Email and SPAM

SPAM is the electronic equivalent of junk mail. That's email you didn't ask for (or agreed to accept without realizing) and almost always don't want. Some SPAM is junk email from legitimate companies trying to sell you their product. Others are junk email from less-than-respectable companies trying to do the same. Taken together, all those spammers eat up a ton of bandwidth.

5.1.1 What Is SPAM?

If you're curious, SPAM is actually a canned meat product. If you haven't had it, the taste is somewhere in between ham and corned beef. However, in computer usage the term SPAM comes from an early 1970's Monty Python comedy skit. In the skit, a couple is trying to order breakfast without SPAM in a restaurant where every meal comes with SPAM in some form. The overall feeling is that **SPAM** is everywhere, in everything, and you just can't escape it. Junk email definitely generates similar feelings.

SPAM Unsolicited email messages, also called electronic junk mail.

A surprising amount of SPAM is for products that are either clearly illegal or on pretty shaky ground. For example, a common source of SPAM is ads for online degree programs. In fairness, there are a number of excellent, highly respected online degree programs—particularly for master's degrees. However, most of these schools don't flood the net with SPAM advertising their programs. The schools that do tend to be—you guessed it—"non-accredited" universities. In evaluating any item or service you find advertised in unsolicited email, remember to "Caveat Emptor." That's Latin for "Let the buyer beware!" At the risk of being obvious, any college degree that you can get over the Internet while attending no classes and taking no tests of any kind is clearly not cool. This type of company is called a diploma mill. A diploma issued by such a school is not a real college degree. More important, using such a fake diploma to get a job or obtain a promotion is illegal.

5.1.2 Isn't SPAM Illegal?

That's a good question without an easy answer. Truthfully, some SPAM is illegal. Some isn't. It's also very difficult to tell the difference. Because SPAM is so disruptive, the U.S. Congress addressed it specifically in the CAN-SPAM Act of 2003, then reviewed and extended that legislation in 2005. So, CAN-SPAM is still in effect (and still ineffective).

Like most government initiatives, this effort was named by an acronym—CAN-SPAM actually stands for Controlling the Assault of Non-Solicited Pornography And Marketing. Its goal was to reduce the amount of SPAM by making senders legally liable. In fact, its definitions actually legalized a good bit of SPAM, leading opponents to begin calling it the "I Can SPAM" Act. What the bill did define as illegal was any unsolicited electronic messages that didn't include a valid subject line and header, the real postal address of the mailer, a clear label marking the content as Adult-only if it was, and an opt-out mechanism.

Felony First

In 2004, Jeremy Jaynes became the first person convicted of felony SPAM. During his peak, Jaynes sent upwards of 10 million messages a day, mostly for "get rich quick" schemes and various fake goods and services.

Sadly, the Virginia law under which he was convicted was later overturned—a reversal that was upheld in March 2009 when the U.S. Supreme Court refused to reinstate the law.

It didn't work. Three years after the passage of this act, SPAM had increased to comprise 75% of all email messages, and less than one half of one percent of those messages actually complied with the provisions of the CAN-SPAM Act.

Interestingly, the first person arrested under the CAN-SPAM Act was a teenager, 18-year-old Anthony Greco of Cheektowaga, New York. Overall, however, arrests under CAN-SPAM have been rare and successful prosecutions even rarer.

The big problem with CAN-SPAM is the opt-out mechanism. An opt-out mechanism is a way for the recipient to get off the mailing list. You've no doubt seen these in junk email that you've received. The general format is:

```
If you would prefer not to receive further information from Spammer-of-Your-Choice,
please reply back to this message with "Remove" in the subject line.
```

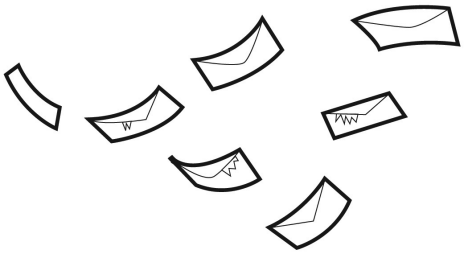
You may also have seen the format:

```
If you would like to stop receiving our advertisements or believe this message was sent
in error, you can visit our subscription management page.
```

To add more substance to their claims of legitimacy, spammers often actually cite the CAN-SPAM Act in their opt-out clauses:

```
This email is a commercial advertisement sent in compliance with the CAN-SPAM Act. We
have no desire to send you information that is not wanted, therefore, if you wish to be
excluded from future mailings, please use the link at the bottom of the page.
```

The general idea is always the same. To get off the mailing list, you need to visit the spammer's website or send them an email. The problem is that as soon as you do so, you have verified that they have a real, valid email address and that their messages are getting through. If the spammer plays by the rules, this works well. If they don't, you have just told them that your email address is worth selling. Because many spammers don't play by the rules, experts strongly recommend that you NEVER reply to unsolicited email or visit links included in SPAM. Doing so can greatly increase, rather than decrease, the amount of SPAM you receive in the future.



5.2 Spoofing

A spoof is a parody of something familiar. In its pure form, a spoof is usually a pretty good joke. Weird Al Yankovic has made a career out of writing musical spoofs of popular songs. One of his best was a 1983 parody of Michael Jackson's hit *Beat It* called *Eat It*. The music video for this one was especially funny.

Email spoofing isn't nearly so funny. **Email spoofing** happens when the person who sends you an email—nearly always a SPAM message—pretends to be someone else. Spammers are able to "spoof" messages by defining fake headers that include phony routing information. Real routing information is the part of your email that defines your email account's Internet address. These are the numbers that allow email servers to deliver your mail. You can think of the routing definition as very much like a postal address. If the address isn't valid, the email doesn't get through. Phony routing information hides the real address of the person sending an email message.

5.2.1 Spoofed Addresses

When you send an email message to someone else, the message sent always begins with a header that includes your name and email address. Those items are defined in your email software as the "Display name" and "Display email address". By changing those settings, you can actually display anything you want. Of course, tracing an email spoofed this easily would be fairly simple. Spammers also insert fake routing information; this makes it appear that the email was sent through one or more systems that most likely never touched it. Tracing messages spoofed with fake routing information is MUCH more difficult and sometimes impossible.

Spoofed email An email message containing a fake From: address making it impossible to tell where it was actually sent from.

One of the reasons that spoofing email is fairly easy is because email headers are created using **SMTP (Simple Mail Transfer Protocol)**, and SMTP lacks authentication. One way to limit spoofing is to use digital signatures with your email. We'll talk about digital signatures in *Chapter 8, Safe Cyber Shopping*.

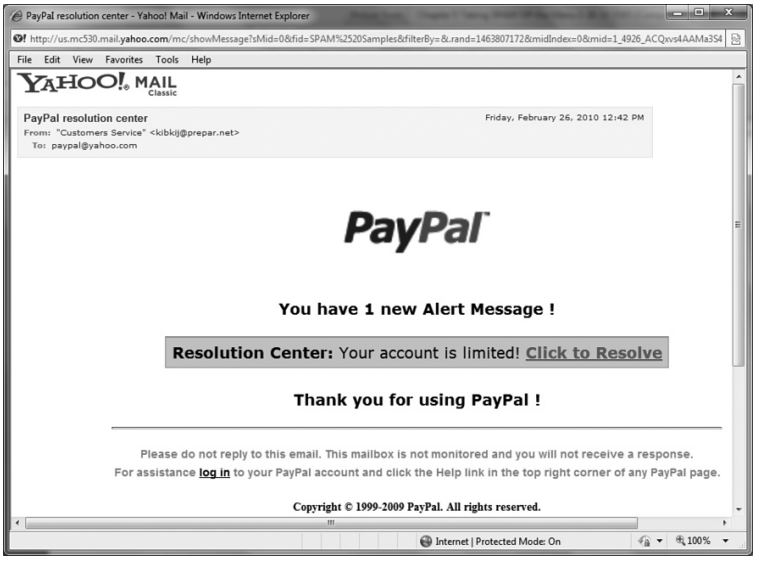
SMTP (Simple Mail Transfer Protocol) The Internet rules used to send and create email messages.

In some cases, spoofed emails are simply amusing. A few years ago, pranksters circulated a very funny election parody that appeared to all the world to have come from the Democratic National Headquarters. It was clearly a joke and the spoofing (while inappropriate) wasn't done in malice. That's not the case for many spoofed emails.

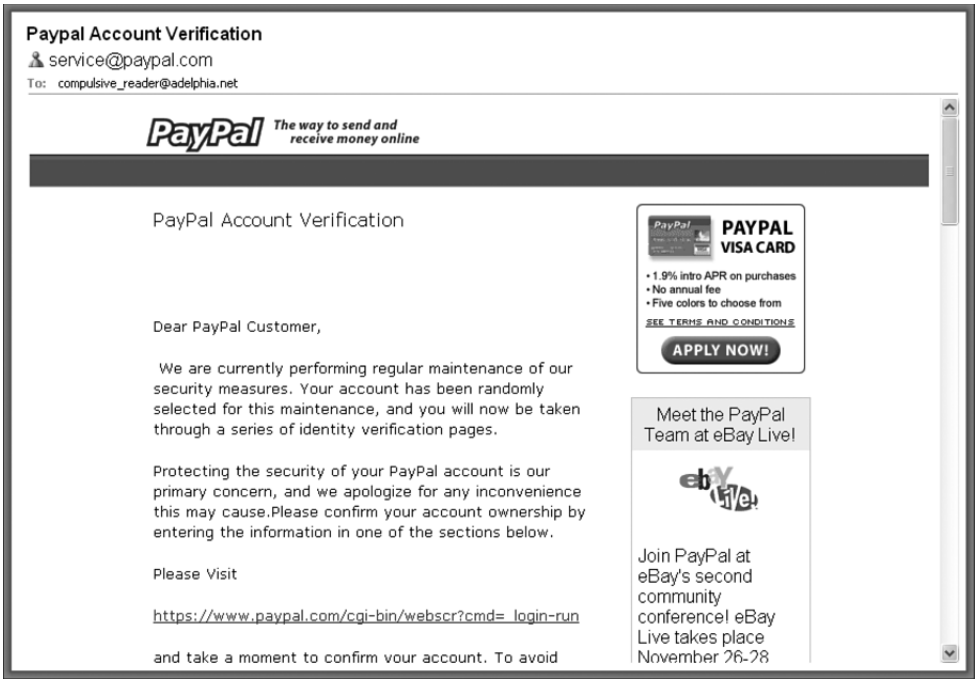
Spoofed addresses are a common theme in phishing attempts. **Phishing** (pronounced "fishing") is a con-artist trick to fish for information. Phishers send email that appears to come from a company you know and trust and asks for information that you would probably want that company to have. At the moment, users of online services like eBay, Amazon, and PayPal are often the targets of phishers. For example, if you or your parents enjoy buying items on auction at eBay, you probably have a PayPal account. PayPal allows you to create an online bank account and use that account to buy items on eBay without giving your credit card numbers to the eBay sellers.

Phishing A con artist scam to trick people into giving out personal and financial information.

If you have a PayPal account, you've probably already received an email something like this:



Or, the more detailed version:



The problem? These emails were *not* sent by PayPal. If you click the included links and enter the information they request, you will be literally giving your parents' credit card information to thieves.

We'll talk more about phishing in ***Chapter 7, Phishing for Dollars***. For now, just be aware that when it comes to email headers, what you see isn't always what you get.

5.2.2 SPAM Proxies and Relays

As you now know, much of the SPAM that is circulating didn't really come from the addresses contained in those emails. What you don't know is that some of it may even have come from your machine.

How can that happen? In Chapter 2, we talked about bot armies and how malware writers can infect your PC with a Trojan program that turns it into a zombie. A lot of those zombies are used to send SPAM. One virus that does this is SoBig.F.

SoBig also spoofs the addresses in the emails it sends so that they appear to come from someone else whose address appears in your email address book.

When a zombie PC is hijacked and used to send SPAM, it's called a **SPAM relay**. That PC is simply "relaying" (passing on) SPAM messages that originated somewhere else. This happens a lot. Unprotected home computers are a major stumbling block in the fight against SPAM.

SPAM relay A hijacked PC that's used to send SPAM without the PC owner's knowledge.

While home PCs are definitely a problem, sometimes so are the mail servers used by Internet Service Providers (ISPs). While fewer servers than individual PCs are hijacked, their extensive databases of email addresses still make them a large problem. When a mail server is hijacked to send SPAM, it's called a **SPAM proxy**.

SPAM proxy An email server that's been hijacked to deliver SPAM.

Today, ISPs are taking great care to prevent their mail servers from being hijacked. Tragically, most home PCs users are not. Luckily, the steps needed to protect your machine from being turned into a SPAM relay are the same as the steps required to protect yourself from computer viruses, worms, and Trojans.

5.3 Knock Knock— How Spammers Know You're Home

Assuming that you haven't been posting your email address all over the Internet, you may be wondering how the spammers find you and why they send you so MANY email messages. That's a good question with a couple of good answers.

5.3.1 Hidden Tracking

Popular belief has it that in the event of a nuclear meltdown, the two groups virtually guaranteed to survive are rats and cockroaches. This applies to the Internet as well. In the event of a total system shutdown, the first groups to resurface are likely to be spammers and web bugs.

If you haven't seen a **web bug**, or even heard of one, you're in the majority. A web bug (sometimes called a web beacon) is a hidden image that spammers use to track email messages. In technical terms, most web bugs are defined as a transparent GIF—a picture file having a size of only 1 x 1 pixel—making them much too small to actually see in an email.

Web bug A hidden image that spammers use to verify that you're actually reading the SPAM they sent you. (Also called a web beacon or transparent GIF.)

When you read an email message, graphics or picture elements in the email are displayed by being downloaded from a separate website. In the past, most email programs were set to automatically download graphics so readers had no idea they were downloading information from another site. Today, that default has been reset so that you'll often see broken images like this:

One by One...

When you look at a picture on your computer screen, you see a solid graphic image—much like a photograph or drawing. In reality, each computer image is composed of thousands of tiny little dots, called pixels.

The term pixel, in fact, is an abbreviation for "picture element." How many pixels a graphic has determines its resolution—how "solid" or crisp the picture looks.

If you use a digital camera, you already understand this term. A high-quality photograph takes an awful lot of pixels. For example, the Kodak Easy Share P880 provides an 8 megapixel sensor. That's eight times roughly 1 million pixels for a single photograph.

Try to imagine a picture that's only one pixel by one pixel. You can't see it, which is of course, the idea of web bug graphics.

If you click to download the graphics the spammer knows that your email address is valid and that you actually read the email message. Don't be surprised if you keep getting spammed!

5.3.2 Scavengers and Crawlers

We kidded above that you might be surprised by the amount of SPAM you get, assuming that you hadn't posted your email address all over the Internet. Amazingly, many people do just that! They use their email addresses as user names for online communities, include their email addresses on their websites, and even use their actual addresses when posting messages to online user groups. All of these steps are good ways to get SPAM.

This is also an area where it's important to lock down your social networking information. Ideally, contact information, like your email address, should be set to display only to Friends, if at all. Truthfully, you don't need to provide email addresses to anyone on social networking sites. Anyone who can find you on Facebook or MySpace can actually contact you via a message or email ON those sites without ever needing your personal address. Obviously, never include your full email address in any messages that you post to someone else's page or wall.

Email scavenger A type of web crawler program that searches the Internet and collects (harvests) all the email addresses it finds posted on web pages.

Posting your email address online can cause problems because some spammers use programs to crawl Web pages (i.e. search them) on the Internet looking for the famous @ sign which appears in virtually all email addresses. Some companies earn fairly decent profits by doing just this.

5.3.3 Is Your Email Address For Sale?

If your email address has been posted on the Internet, chances are that someone is selling it right now. Because the Net is a public place, harvesting addresses for sale (although annoying) is a perfectly legal endeavor. If you run a quick web search on "email harvester" or "email spider," you'll find a wide variety of products that harvest email addresses, most priced well under $100.

Sometimes, sellers don't need to "harvest" email addresses. They simply use their own customer or member records. In 2009, music service SpiralFrog sold the addresses of its 2.5 million customers to multiple spammers literally days before creditors took control of the now defunct firm. One of those spammers paid $8,500 for the addresses. While that was, as a former SpiralFrog customer noted, "Slimy", it probably wasn't illegal. Many free (and paid) service providers reserve the right to share, distribute or sell the information you provide them. That's why it's important for you to read each website's privacy policy before you provide that information.

5.4 Social Engineering

Strangely, some scammers focus on SPAM because people like you are beginning to get smart and protect their machines with applications that keep hackers from targeting software vulnerabilities.

Most SPAM messages rely on social engineering to trick recipients into reading the email. These are some of the same tricks that virus writers use to get you to open email attachments when you know you really shouldn't.

For social engineering purposes, spammers rely heavily on the displayed `From:` and `Subject:` fields in the email messages. Often, `From:` fields are spoofed to appear to come from companies or organizations you know and trust. The `Subject:` lines are written to catch you off-guard or play on curiosity or greed.

Here are some of the more common subject lines that spammers use:

```
Subject:  RE: About your email
```

This approach tries to catch you off-guard and trick you into thinking that this message is a response to an email you sent. Don't assume that every email that begins RE: is really a reply. Always look at the `Sender:` field.

```
Subject:  Free Xbox games for 30 days
Subject:  Sweepstakes PRIZE Notification – You WON!!!!
```

Free stuff is always great, isn't it? Since many teens enter online sweepstakes and contests, this is a very effective approach. When you receive an email like this, ask

yourself whether the prize matches up with any sweepstakes you really entered. You also might want to be careful about entering all those sweepstakes. Many exist solely to harvest email addresses.

```
Subject: Lose up to 50 pounds in one month!
```

Weight-loss SPAMs are strangely effective with young people. A 2009 study published in the *Southern Medical Journal* found nearly 20% of overweight college students actually bought weight-loss products marketed via email SPAM. Unfortunately, most products advertised via SPAM are more likely to lighten your wallet than anything else. The person to ask for weight-loss help is your doctor, not your neighborhood spammer.

5.5 Keeping Spam Out of Your Inbox

When spammers first started gaining ground, there really weren't enough good tools to keep them out. Today there are many sophisticated tools and techniques for blocking SPAM. The way you use your email address and the actions you take when SPAM gets in are both important components in keeping SPAM out.

Even though technology to block SPAM is getting better, spammers are always trying to work their way around it. No method will protect you from 100% of SPAM. Still, your first line of defense is to do the following:

- Delete suspicious email without reading it!

  This is a good way to avoid viruses and worms as well as more SPAM.

- Don't click on links in your email.

  Remember the web bugs? Don't let them crawl into your PC!

- Don't reply to SPAM.

  While a few opt-out mechanisms are really legitimate, an awful lot more of them aren't. In the long run, you'll get less SPAM if you just delete it than if you ask to be removed from the mailing list.

- Watch where you post your email address.

  To avoid being caught by web crawlers collecting email addresses, don't post your full email address on any publicly-accessible web page.

- Use filters if you have them, but don't trust them to do the whole job.

  Filters can be a useful tool in avoiding some types of SPAM. But spammers are constantly rewriting their subject lines to avoid being thrown away by filters. Often, message content is contained in a graphic/picture file. Since filters scan text, they miss any key words or phrases contained in graphics.

5.6 SPIM

SPIM is the instant messenger version of SPAM. Like SPAM, it proliferates wildly and greatly annoys its recipients.

Distribution of **SPIM** has grown with the use of instant messaging. In 2007, about 50% of American teens used instant messaging. By 2009, that figure exploded as social networking members took advantage of the IM features of Facebook and MySpace.

SPIM Unsolicited instant messages. SPIM is the IM version of SPAM.

Teens use instant messaging even more heavily than adults. As a result, they are even more likely to receive SPIM. Sometimes, that SPIM is even intentionally targeted at teens. In February of 2005, an 18-year-old New Yorker, Anthony Greco, became the first person arrested for sending SPIM after he flooded MySpace.com with roughly 1.5 million SPIM messages. Anthony literally overwhelmed those users with SPIM ads for mortgage refinancing and inappropriate adult sites. If you're thinking that he couldn't have expected much click through on the mortgage ads, you may have missed the point. Anthony's real goal wasn't to sell the services being SPIMmed; it was to extort money from MySpace. He actually contacted them and offered to protect their users against SPIM for a mere $150 a day. That turned out not to have been his brightest move. Greco was arrested at the Los Angeles airport where he thought he was flying out to meet Tom Anderson, president of MySpace,

to sign a payment agreement for the extorted funds. Some criminals just don't think it through.

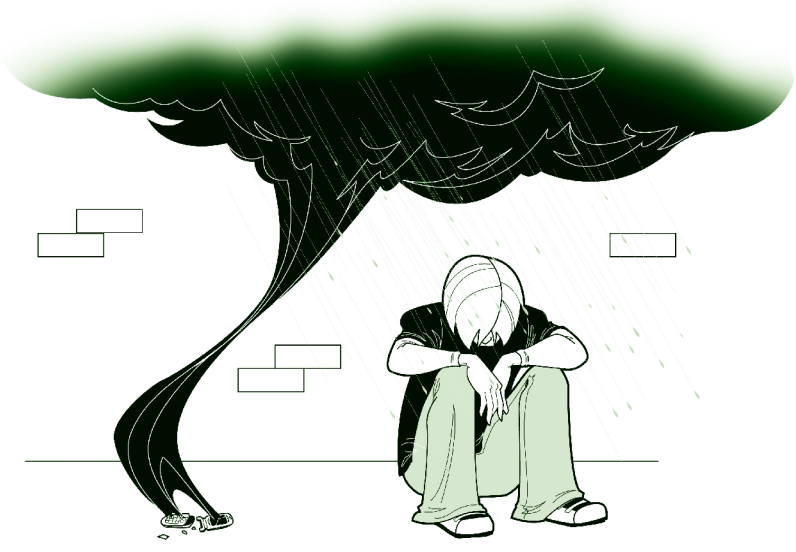
SPIM, like SPAM, also often exists to redirect users to malware sites. In May 2009, Facebook users were inundated with messages asking them to "look at mygener.im." Users who clicked on that link were directed to an adware website.

Frequent targets of both SPIM and SPAM, the social networks are beginning to fight back with lawyers as well as security updates. Recently, Facebook was awarded a $711 million judgment against so-called "spam king" Sanford Wallace for his attacks on Facebook users. While Wallace is unlikely to ever pony up that much cash, the civil suit marks a new aggressive stance by social networking sites against spammers.

Chapter 6

Cyberbullies

Megan Meier, a 13-year-old from Dardenne Prairie, Missouri, met 16-year-old Josh Evans online at MySpace. In a few short weeks, the two became close friends online, although they never actually met in person. Josh claimed to have recently moved to the nearby town of O'Fallon where he was homeschooled and didn't yet have a phone. Still they corresponded online often and Megan's family reported her in good spirits. But after a few weeks, what began as an online flirtation turned nasty. Josh reported hearing that Megan wasn't very nice to her friends. He reposted Megan's messages without her permission. Hurtful comments about Megan were posted online. Then Josh sent a final message stating that, "Everybody in O'Fallon knows how you are. You are a bad person and everybody hates you... The world would be a better place without you." Shortly after that, Megan committed suicide.



Megan's experience was tragic—even more so because Josh Evans didn't actually exist. The MySpace account using his name was created by 49-year-old Lori Drew, the mother of a former friend of Megan's who lived just four houses away. Prosecutors discovered that the hurtful messages were sent by Drew and her then 18-year-old temporary employee, Ashley Grills. In addition, Lori Drew was fully aware that Megan was being treated for depression before she initiated the hoax.

In response to Megan's death, cyberbullying has become a nationally recognized problem. WiredSafety has initiated a program to encourage teens to take **Megan's Pledge** and also agree not to "use technology as a weapon to hurt others."

Sadly, Megan is far from the only teen harassed beyond endurance by cyberbullies. Nor is MySpace the only venue for attacks. On January 14, 2010, 15-year-old Phoebe Prince of South Hadley, Massachusetts committed suicide after a year of cyber attacks via text message and Facebook by a group of girls at her school. If you think only girls are targeted by cyberbullies, think again. Boys are also at risk, as was evidenced by the suicide of 13-year-old Ryan Patrick Halligan of Vermont, who had suffered months of cyberattacks by bullies questioning his sexual orientation. In 2008, a 16-year-old Brighton boy barely survived a suicide attempt following an extended "relationship" with what turned out to be a fictitious boy named Callum on the networking site Bebo.

What all of these teens had in common was a vulnerability to betrayal and humiliation from online Friends who weren't what they appeared to be.

6.1 Bullies Go Digital

School yard bullies have been an issue since the days of the one-room school house. Today, those bullies simply have a larger venue and a lot more victims to pick from. The term **cyberbullying** covers a wide range of harassing behaviors. Cyberbullying often includes posting hateful messages on social networking sites that reach hundreds of local kids. In the past, it simply felt like bullies could trash your reputation to nearly everyone at school. Today, with kids having literally hundreds of online Friends, those same bullies really *could* reach nearly everyone at school.

Cyberbullying isn't limited to computers either. It can also include sending harassing text messages and inappropriate photos via cell phone. Sometimes, kids upload those texts from cell phones to websites, expanding their audience and furthering the damage.

Cyberbullying A form of intimidation and harassment using electronic means such as email, text messages, chat rooms, and social networking sites.

Cyberbullying can take many forms. Some bullies attack by sending insulting or threatening emails or cell phone text messages. Others attack on social networking sites by creating hate groups. A few attack in multiple formats at the same time, leaving their victims feeling constantly under siege. One teen reported being bullied by an ex-boyfriend on Facebook, MySpace, and Bebo, by email, on Twitter, in YouTube videos she didn't authorize, and even through text messages. Eventually, she was afraid to turn on her computer or answer her phone.

> I hate u everyone hates u...
> u should just die.
> *—Anonymous posting to a teen's website*

Other bullies are less persistent but astonishingly mean. Some bullies have used online polling sites to create contests for the fattest or ugliest person in their school. Sadly, today's technology provides ample opportunities for anonymous cruelty.

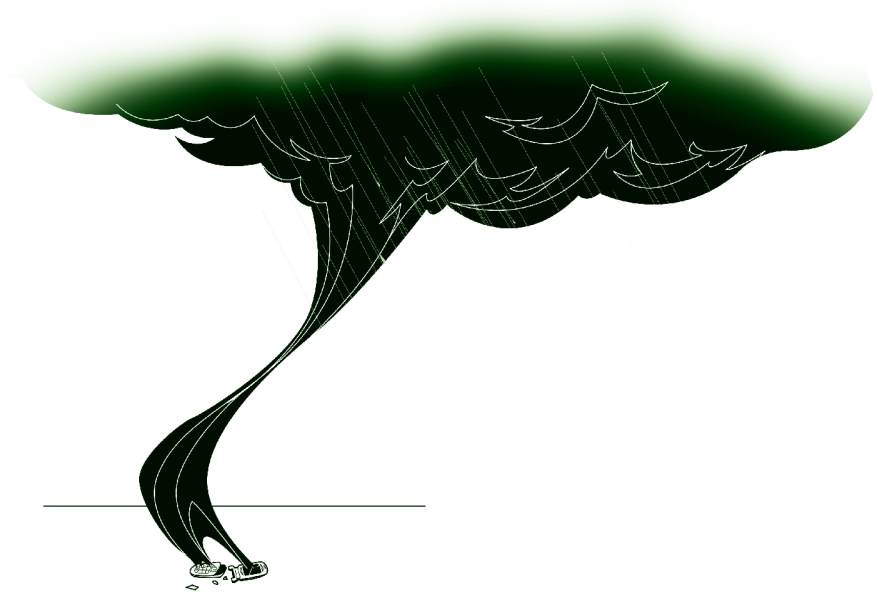
How bad is it? Over half of middle-schoolers have been bullied online at least once. And just about every teen we talk to either knows someone who has been bullied, or has been bullied themselves.

6.2 Online Reputation Attacks

The most common form of cyberbullying is the online reputation attack. Your online reputation is important. Unless you're planning to step back from the 21st century altogether, a sizeable portion of your life will be spent, discussed, and recorded online. At some point, your Friends may outnumber your friends. At the very least, you're going to have some heavy cross-over between your real and virtual worlds. A bad reputation in one is bound to have repercussions in the other. For this reason, online reputation attacks are the primary method of attack used by cyberbullies.

6.2.1 Frontal Assaults

Most online reputation attacks by cyberbullies are pretty straight-forward. A common attack is the social networking hate group. This consists of a social networking site group or other web page that is literally entitled "I Hate John Doe." Not terribly original, but we've already established that cyberbullies aren't very bright.



A quick scan of social networking groups revealed literally thousands of hate groups. One group that really exemplified the concept was the Facebook group named "I hate Jeremy _____ ." We're being delicate here, of course. The real group name listed Jeremy's complete first and last name. It also had photos of Jeremy, the name of his high school, and status postings announcing," I hate Jeremy, how about you?"

Clearly, the Jeremy hate group was an incidence of cyberbullying. How can we tell? First, there's the obvious "I hate" naming scheme. Another clue is that the administrators and nearly all members of the group attended the same high school. Interestingly, the Profiles of Jeremy's haters seemed especially lame. Jeremy, on the other hand, seems to be an intelligent, well-behaved kid. In twenty years, those cyberbullies may very well be bringing Jeremy's coffee or flipping his burgers. Of course, that won't affect how badly Jeremy may feel today.

Technically, of course, hate groups aren't allowed. Virtually all social networking sites explicitly ban this type of group. The Jeremy hate group actually violates three of the Facebook terms of usage where users agree not to harass other users, not to post content that is hateful, and not to encourage others to violate the terms of usage.

So why doesn't Facebook automatically remove hate groups? Surprisingly, that's not as easy as it sounds. There are many people, places, and things that it's perfectly okay to hate online. For instance, there are many long-time members of the group "I hate Brussels sprouts." It's also okay to hate television shows, movies, and musical groups. Based on the number of fan groups and hate groups, Facebook users obviously have a serious love/hate relationship with the *Twilight* films. Individuals are also fair game IF they happen to be public figures. This includes politicians, although you should definitely use common sense in your posts there. While it's within your first amendment rights to hate any elected official, if you're even thinking about making any empty threats, remember that the FBI, CIA, Secret Service, and NSA all have people scanning the Internet for potential threats to national security.

6.2.2 Identity Assaults

Identity assault, like identity theft, occurs when someone else pretends to be you. The difference is why. With identity theft, the perpetrators impersonate you in order to get something for themselves. That might be a credit card they don't need

to pay for (since you'll be blamed for the bill). Or it might be a social security number they can sell to an undocumented worker. The point is that identity thieves don't actually care about YOU. They want your identity for what THEY can get out of it. Identity assault, on the other hand, is ALL about you.

In an identity assault, the cyberbully impersonates you in order to trash your reputation. Bullies often create websites in their victims' names, then fill those websites with hateful speech or content. The idea is to make anyone who reads the website think that you're a terrible person. A city judge in Ohio fell victim to this type of identity assault when a criminal he'd sentenced earlier created a web page in the judge's name that portrayed him as a racist pedophile. The bully doesn't need to create pages either. He or she can just use your real name and address to register at sites that promote drug use, pornography, or any other issue that would make you look undesirable to a college admissions officer, potential employer, or recruiter who was researching your identity online.

Most cyberbullies stick to insulting and threatening their victims. However, a small number actually commit crimes on behalf of their victims. In 2007, an Internet crime fighting group called CastleCops was attacked by someone who flooded their PayPal account with donations from scammed PayPal accounts. The PayPal victims knew nothing of the intermediary. All they saw was that their accounts had been ripped off and that the money was routed to CastleCops. The damage to CastleCop's reputation was substantial.

6.3 Reputation Management

Your online reputation is more important than you probably realize. Most employers routinely check online postings of job candidates. A reputation smear in high school could affect your earning potential 10 years later. To prevent problems, your best bet is to monitor your online reputation and move quickly if you find any problems.

6.3.1 Google Yourself

To protect your online reputation, you need to know what people are saying about you online. One way to do that is to Google yourself. (Or Yahoo! Or Bing. Any of the major search engines will work. Since they don't always look the same places, it might even be good to search yourself using more than one search engine.)

The downside to Googling is that it doesn't work well for people with incredibly common names. John Smith returns 100,000,000 search results. Unless your given name or surname is incredibly uncommon, the chances are that you'll need to search for more than just your name. The plus side is that if your name is that common, no one is going to assume that the John Smith registered as an aspiring neo-Nazi is really you and not some other John Smith.

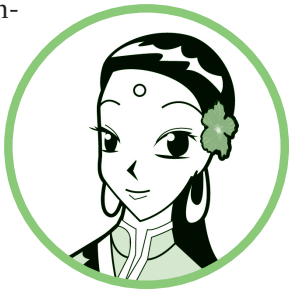
If your name is fairly common, you'll want to search for your name AND city or your name AND phone number, etc. Also search for your email address.

6.3.2 Call in the Professionals if You Need To

If you find that your online reputation has been compromised, you'll want to do something about it as quickly as possible. Even if it doesn't seem important now, it may become very important in a few years when you look for your first job. According to a Cross-Tab report, 70% of recruiters have rejected candidates based on information found online. If you're going to be rejected based on something online, it should at least be something *you* actually did or said, not something posted by a cyberbully to make you look bad.

Your first response should be to complain directly to the site on which you found information damaging to your reputation. Most sites promptly remove any postings that might be construed as harassment.

If that doesn't work, consider contacting a professional. A number of companies actually specialize in reputation clean-up. Defendmyname, Naymzma, and ReputationDefender are just a few. Don't expect miracles though—and do expect a substantial price tag. Monitoring services, which search the Internet for potentially damaging posts by you and about you, are quite reasonable at around $10 to $15 a month. However,



that just FINDS the nasty stuff about you. Actually removing that information costs upwards of $30 per item.

While you're notifying professionals, don't forget to notify law enforcement professionals if appropriate. Otherwise, you could end up with the same problem as this teen who posted to Ask.com on Yahoo!

6.4 Protecting Yourself from Cyberbullies

While reputation clean-up is possible, it tends to be difficult and expensive. It's much better to protect yourself from cyberbullies in the first place than to try to undo the damage they can do. Like most areas of computer crime though, that protection is hard to come by.

When the "MySpace Mom Suicide" story broke, public attention was immediately focused on the issue of cyberbullying. Since then, the case has served to illustrate the difficulties of legally protecting kids from online harassment, even blatantly harmful harassment as in this case. Initial public reaction to Megan's suicide was followed within a year by criminal prosecution. In November 2008, 49-year-old Lori Drew was convicted in what legal experts consider the first official prosecution of cyberbullying. That conviction was based on Drew having violated the MySpace terms of service which require users to provide factual information about themselves, and to agree not to use the service "to harass or harm other people." In July 2009, however, that conviction was overturned on the grounds that the

parties involved never actually read the terms of service before clicking the button to agree to them. (We discussed earlier how malware writers count on users not reading EULAs in order to "legally" dump unwanted adware. Apparently, cyberbullies are also protected by users agreeing to terms they haven't read.)

The Drew case also led to the introduction of the Megan Meier Cyberbullying Prevention Act. However, as of 2009 that bill was stalled in committee. Several media outlets reported serious problems with First Amendment Rights in the proposed bill. That's likely to remain an issue with any laws regarding cyberbullying. It's nearly impossible to protect Free Speech, as our society strives to do, without at least sometimes protecting hateful speech as well.

So what can you do to help? If you know about a cyberbullying incident at school, report the abuse—even if it's not you being targeted. Make it a personal crusade not to tolerate cyberbullying. Remember, a crusade can be started by anyone, anywhere. After Megan Meier's suicide, a group of teens began a crusade to stop cyberbullying as a way to honor Megan's memory. They created Megan's Pledge, a commitment by teens to work against cyberbullying. Consider involving your school in their crusade.

What else can you do to protect yourself and your friends from cyberbullies? Be vigilant and mind the top ten steps to prevent cyberbullying:

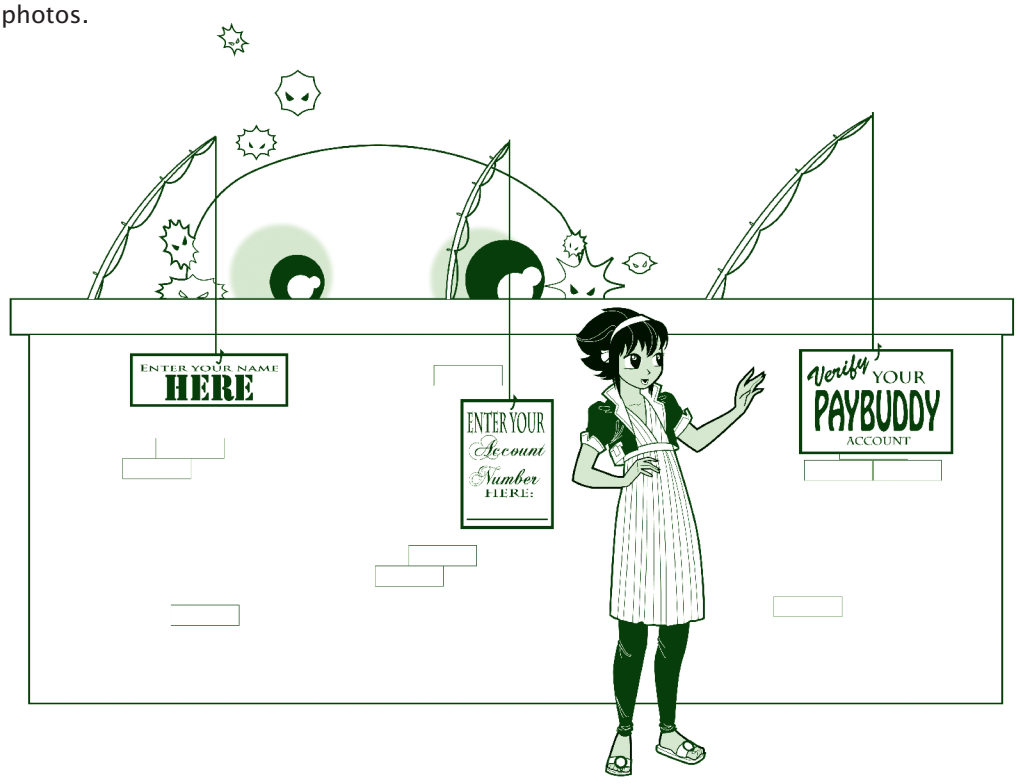
1. **Know your Friends.** Some teens put themselves and their information at risk by accepting people they don't actually know as online Friends. They seem to believe that everybody does this. That's not true. A 2008 study of teen social networking site users by University of California researchers found that only 5% of teens had online friends they didn't actually know offline. So feel more comfortable next time you *Ignore* a Friend request from someone you don't recognize.
2. **Sign Megan's Pledge** and encourage your school to have every student sign the pledge. Don't forget that cyberbullying attacks are successful because other kids hop on board and become attackers rather than rallying against the attackers. You can download the pledge kit from stopcyberbullying.org.

3. **Limit the information you post.** Never include personally identifying data like your home address or phone number. This can protect you from identity assault.
4. **Set your Privacy settings carefully.** Social networking sites now allow you to designate privacy settings on virtually everything you post—status updates, photos, group memberships—as you make those postings. Carefully consider how public you want to be about your private life. Don't think just because you set your page to private that it cannot be accessed.
5. **Know what your Friends post about you**—in photos as well as in words. Your friends may not be as concerned with protecting your privacy as you are.
6. **Trust your instincts.** If a new Friend begins to creep you out, unFriend them. Fast.
7. **Think *before* you click.** Don't forget that you can't take something back once you hit send or post. If you're not sure whether something's appropriate, it's probably not. Be especially careful about posting anything when you're mad or upset. If you find yourself seething about something you've read online, take a break away from your computer before you respond.
8. **Report abuse.** Actions online can do more than hurt. Reporting abuse might even prevent a suicide. How would you feel if you knew and DIDN'T say anything? Is that something you want to carry around with you for the rest of your life?
9. **Don't bully yourself.** Think carefully before each and every post. Too much online reputation damage is self-inflected when people post first and think later.
10. **Don't bully others.** Treating others the way you want to be treated is *never* a bad decision. It will also protect you from cyber attacks in retribution.

Chapter 7

Phishing for Dollars

In May 2006, 14-year-old Takumi of Nagoya, Tokyo became the first Japanese minor charged with the Internet crime of phishing. Takumi tricked users into divulging personal information by creating a website that he disguised as a popular Internet gaming site. Using this ploy, Takumi stole the identity of 94 people. He even tried to blackmail teenage girls from whom he'd stolen personal information into sending him naked photos.



The only thing unusual about Takumi was his age. Because there's so much money at stake, phishers these days tend to be professional thieves. The Russian mafia and other organized crime groups take phishing seriously. So should you.

This chapter discusses phishing scams in detail. It tells you how to spot a phishing expedition and how to avoid being hooked. For their own good, that's a skill you'll want to share with your parents.

7.1 What Is Phishing?

Phishing (pronounced "fishing") is just what it sounds like—con artists fishing for information. A phishing attack generally begins with a spoofed email. That email pretends to be from a company you know and trust and possibly already do business with. The email claims there's a problem with your account, potentially fraudulent use or charges, or simply asks you to verify your information to help them to protect you. That's actually a nice bit of social engineering—the con artist offering to protect you from security risks.

Phishing An attempt to trick users into revealing personal information or financial data.

Probably one of the best-known phishing attempts is the PayPal scam.

If you've used the Internet to buy anything at auction, you're no doubt familiar with PayPal. PayPal is the online service that people use to pay for items that they purchase on sites like eBay. While it's not technically a bank, PayPal functions very close to a bank—allowing you to transfer money easily to any other PayPal user by simply sending an email message. Those types of transfers are possible because when you (or your parents) set up your PayPal account, they linked that PayPal account to an actual bank account or to a credit card.

Online shoppers like PayPal because it feels safer than handing out credit card numbers to perfect strangers. So what's the problem? In recent years, PayPal has also become a major target for hackers and phishers. And they're not alone. While we've talked about denial of service (DoS) attacks and worms aimed at taking out commercial websites, the biggest problem to hit most of the big online

players—like PayPal, eBay, and Amazon—really hasn't been security issues on their sites. The biggest problem has been phishers scamming financial details from their customers.

If you've ever used PayPal, you've probably already been hit by this scam. Even if you've never used PayPal and don't even have a PayPal account, you've probably been hit by this scam. That's because phishers are a lot like spammers. They go for quantity, not quality. PayPal has over 202 million users operating in 190 countries and regions, so chances are that a good percentage of email addresses that phishers SPAM are going to actually be PayPal customers. Do they bother to check? No.

The PayPal Scam

```
Dear PayPal Customer,

We are currently performing regular maintenance of our security measures. Your
account has been randomly selected for this maintenance, and you will now be taken
through a series of identity verification pages.

Protecting the security of your PayPal account is our primary concern, and we
apologize for any inconvenience this may cause.Please confirm your account ownership
by entering the information in one of the sections below.

Please Visit
https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

and take a moment to confirm your account. To avoid service interruption we require
that you confirm your account as soon as possible. Your account will be updated in
our system and you may continue using PayPal services without any interruptions.

If you fail to update your account, it will be flagged with restricted status.

Thank you,
The Paypal Staff
Thanks for using PayPal!
-----------------------------------------------------
PROTECT YOUR PASSWORD

NEVER give your password to anyone and ONLY log in at
https://www.paypal.com/cgi-bin/webscr?cmd=_login-run Protect yourself against
fraudulent websites by checking the URL/Address bar every time you log in.
```

This also explains why your parents may have gotten requests to "update information" for credit cards they don't actually hold. Phishers, like spammers, are just playing the numbers. If even a small percentage of consumers take the bait, they clean up.

You'll notice that our sample PayPal scam email asks you to visit a specific webpage, https://www.paypal.com/cgi-bin/webscr?cmd=_login-run. This is a common component of any phishing attempt, the embedded link. At some point, the phishing emails all ask you to click the link provided to log into your account and update or verify your account information. The problem, of course, is that the link doesn't take you to your actual account. Instead, it routes you to a fake screen—often a series of fake screens—that have the same look and feel as the actual company website.

If you follow the link, anything that you type from that point forward is sent directly to the con artist responsible for the phishing attempt. If you enter a user name and password, you're giving that con artist everything he needs to impersonate you on that site. When the phishing target is a bank or bank-like account such as PayPal, you're giving the criminal all the details he needs to literally empty your accounts. If you enter credit card information, you should expect some unexpected charges to follow shortly. While it's possible that the phisher might go on a buying spree with your account, it's more likely that he'll sell your credit card to somebody else. In 2009, valid credit card numbers were selling for around $30 a piece on the black market.

You may even be providing all the data that crook needs to successfully steal your identity. If that happens, new charges on your accounts may be the least of your worries. A savvy thief could open NEW charge cards in your name, littering your credit report with unpaid accounts that could destroy your financial history before you've had a chance to even acquire one.

Email isn't the only method used for phishing. The basic phishing scam actually predates computers by many decades. The big change here is that computers make it easier for the con artists to hide. Unlike phishing by phone, which is easily traced, phishing via email is much easier to get away with because email created using spoofed addresses and fake routing information is nearly impossible to trace.

7.1.1 How Common Are Phishing Attacks?

Incredibly common. In the first half of 2009 alone, there were over 56,000 separate phishing attacks. Some targeted financial data—banks, credit cards, and PayPal are frequent targets. Others targeted seemingly unimportant sites like photo galleries, gaming sites, Twitter, and Facebook. Why? With non-financial sites, what the phishers are really looking for are passwords. While some phishers might really want to steal your World of Warcraft game, most assume that like most people you're overwhelmed by multiple accounts and so using the same sign-in data from one site to another. That user name and password for a seemingly unimportant account may very well work with your bank account.

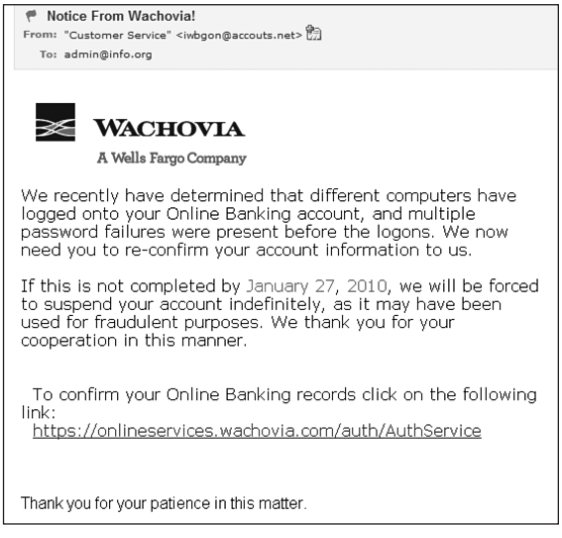
Why are these attacks so common? From the phisher's point of view, the tactic works. While people are becoming a bit more savvy (or perhaps just apprehensive), far too many still fall for the phishing lures.

7.1.2 Who Gets "Phished"?

Although it's individual customers who are hooked, the victims of phishing also include all those companies whose customers lose confidence, and in some cases, even stop using their online services. These include all types and sizes of businesses, but the major victims are online services and financial groups.

Banks

For obvious reasons, banks are major targets in phishing scams. David Jevans, chairman of the Anti-Phishing Working Group (APWG), reported in December 2009 that, "Recently in the U.S. we have seen cybercriminals attempt to steal $100 million from corporate accounts, with $40 million being irrecoverable." That $40 million loss was from corporate accounts guarded by trained financial experts. Just imagine the overall damage to consumers without fraud-prevention training.


Notice From Wachovia!
From: "Customer Service" <iwbgon@accouts.net>
To: admin@info.org

WACHOVIA
A Wells Fargo Company

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us.

If this is not completed by January 27, 2010, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

To confirm your Online Banking records click on the following link:
https://onlineservices.wachovia.com/auth/AuthService

Thank you for your patience in this matter.

Banking scams are similar to other phishing expeditions in that the goal is to trick you into entering your login credentials. Threatening to block access to your account if you don't respond nearly immediately is common. The thieves don't want you to stop and think before you click. The Wachovia email shown here was sent January 26th, threatening to cut off service to non-respondents the next day. A real bank would never give you only 24 hours to respond. Any time you see a demand that you respond insanely quickly, assume that you're reading a scam. In this case, there was no chance of the woman who received this email actually clicking through because she doesn't even have an account with Wachovia. However, Wachovia's a really big bank and many people do.

Because the recipient here recognized the scam, this particular phishing expedition failed. Successful scams cost banks a small fortune in the costs required to cancel accounts and reissue new credit cards. As a good faith gesture, customers receive new cards free of charge. Eventually though, we all pay in higher credit card costs.

Online Companies

Because online businesses often depend on email as their only method of communicating with customers, these firms are hit hardest by phishing scams. The largest online firms, like eBay, PayPal, and Amazon are targeted often.

The Unemployed

Some of the scammers are both fearless and heartless. As the economy tanked in 2009, phishers targeted the unemployed. Tabitha, a 22-year-old recent college graduate looking for work, found that when applying for jobs listed on Craig's List, she received one phishing attempt after another. The emails claimed that job applicants needed to be "vetted" for consideration first, providing a link to a "credit screening" service where the unemployed were asked to input everything a scammer would need for identity theft.

Probably You

There's little reason to believe that you won't land on the scammers' lists in the near future. Are you one of the 125 million users who've been to MySpace? If so, you may have already been phished and not know it. In early June 2006, a spoofed

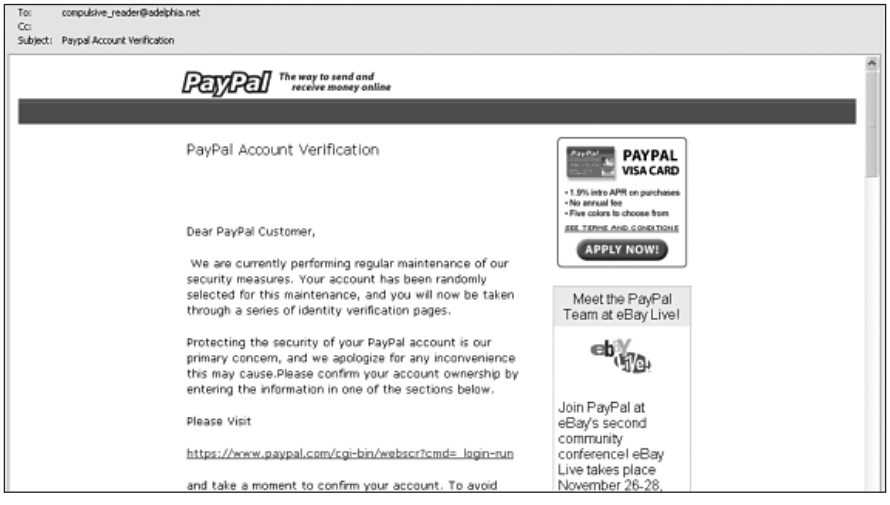
site phishing for MySpace.com logins was discovered and removed in California. An *especially* sly attack, the hacker used IM to send invites to view photos that appeared to come from one of the target victim's online "Friends." If the target bit and used the embedded link provided, he was really entering his login details to a fraudulent site that captured that login information while passing it on and using those details to really log him onto MySpace. The time lag was minimal and the user really ended up at MySpace, so most victims never realized their information had been stolen.

7.2 How to Recognize a Phishing Trip

No one likes being taken for a ride. To avoid being pulled into an unwanted phishing trip, you need to understand two things. First, you need to realize just how good and how convincing the fakes are. Second, you need to know how to spot the phonies.

7.2.1 How Good Are the Fakes?

The fake screens can be very convincing. Check out this phishing attempt to trick PayPal users into revealing their user names and passwords.


To: compulsive_reader@adelphia.net
Cc:
Subject: Paypal Account Verification

PayPal The way to send and receive money online

PayPal Account Verification

Dear PayPal Customer,

We are currently performing regular maintenance of our security measures. Your account has been randomly selected for this maintenance, and you will now be taken through a series of identity verification pages.

Protecting the security of your PayPal account is our primary concern, and we apologize for any inconvenience this may cause.Please confirm your account ownership by entering the information in one of the sections below.

Please Visit

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

and take a moment to confirm your account. To avoid

PAYPAL VISA CARD

• 1.9% intro APR on purchases
• No annual fee
• Five colors to choose from

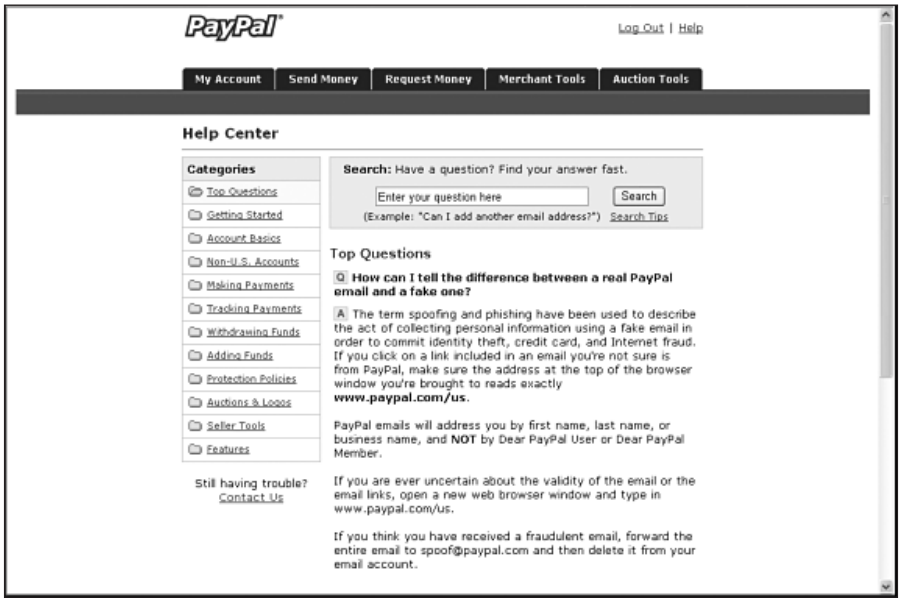
APPLY NOW!

Meet the PayPal Team at eBay Live!

Join PayPal at eBay's second community conference! eBay Live takes place November 26-28,

Fake PayPal screen included in phishing attempt

The fake screen is pretty convincing, isn't it? Notice the ads for PayPal Visa and eBay. Now compare this to an ACTUAL PayPal screen (in this case, appropriately, the Help screen to tell users how to recognize fake PayPal emails and avoid being taken in).



Actual PayPal screen

The spoofed messages themselves are so convincing that up to 20% of recipients respond to them. That's a lot of people putting their personal and financial data at risk. Because of the high frequency of these attacks, many Internet security products do scan for phishing attacks. However, there's always a short gap between a new method of attack and the corresponding new security protection. To protect yourself during that gap, you need to be savvy about recognizing phishing attacks and stay proactive about protecting your personal information.

7.2.2 How Can I Recognize a Phishing Scam?

In *Harry Potter and the Prisoner of Azkaban*, J. K. Rowling introduces a wonderful device called a sneakoscope. While tuned to look mostly for dark magics, the general idea is that the sneakoscope goes off when it encounters persons or things basically up to no good.

Once you know what to look for, it becomes easier to spot the fakes. Quite a number of features tend to give away the fakes. These include use of generic names, a logo that doesn't quite match, poor grammar, verification requests, and masked web addresses. The appearance of any ONE of these items should set off your internal sneakoscope.

Do I Know You?

As Shakespeare put it so eloquently in *Romeo and Juliet*, "What's in a name? That which we call a rose by any other name would smell as sweet." That may be well and good for flowers, but via email what the message sender calls you lets you know, in large part, who it is you're really talking to.

With phishing scams, the spammed email nearly always begins with some euphemism filling the space where your name should be.

Dear Online Service user:

Dear Bank customer:

Dear Credit Card account holder:

Dear Personal Club member:

Sometimes, the scammers try to make this less obvious by omitting "Dear" and beginning with a salutation that doesn't normally require a name:

Greetings!

Welcome!

Warning!

Security alert!

With very few exceptions, any valid email you receive requesting additional information is going to come from a company that knows you as well as you know it. Your bank actually knows your first and last name. So does the company that issued your parents' credit card.

Because of the high incidence of phishing attempts, many companies are now adding names to what would once have been basic form letters. When a friend who buys and sells books online received a generic form letter from eBay addressed to "Dear Half.com user:" she knew that the email actually came from eBay because it also contained the following line above the form letter salutation:

```
eBay sent this message to Melinda J Smith(missy_bookseller).
Your registered name is included to show this message originated from eBay.
```

Using Goodly Grammar

If your mother's like most, she probably reminded you a thousand times to pay attention to your grammar to avoid sounding shallow or ignorant. She might also have added criminal.

For reasons that almost defy comprehension given the easy availability and use of grammar checkers, most phishing letters contain bad, if not downright awful, grammar. Consider this extract from a phishing email sent to Amazon users:

```
Greetings!
Due to simultaneous fraud attempts we received. We regularly update and verify our
customers. During a random review by our department there was a problem in your
account that we could not verify your account information. Either your information
has changed or it is incomplete.
```

What's wrong with this paragraph? For starters, the first sentence is a fragment. "Due to simultaneous fraud attempts we received." While that first sentence stops short, the third sentence continues too far and becomes a run-on. The fact that this scam was directed at Amazon was a nice touch of irony. Do you really think that the world's largest bookseller is incapable of writing a coherent sentence? This is a good example of why you need to pay attention in your English class!

The Devil Is in the Details

A near constant in phishing attempts is the request that you "verify your account" or "confirm your account information." In essence, the con artist wants you to provide all the details that would allow him to use your account.

Because of privacy regulations, security issues, and plain old common sense, legitimate companies will NEVER ask you to verify the following types of information:

- Pin numbers
- User names
- Passwords
- Bank account numbers
- Credit card numbers

Know Where You Are Going?
Another dead giveaway that you're being directed to a fake website is mismatched **URL**s.

URL Uniform Resource Locator. The URL is the word-like address used to locate a specific web page on the Internet.

In the case of phishing attempts that try to trick you into going to a fake website, you'll sometimes find that the URL printed in the email message won't match the actual URL. Often, the fake URL will contain extra letters or words that aren't part of the real web address. This is just one reason that you need to make it a point NEVER to click on links that come embedded in unsolicited emails.

In some cases, the address will look official but still not be right. For example, the PayPal scam earlier in this chapter sends victims to the URL www.paypal-transactions.com. While that looks official, that's NOT the same as www.paypal.com. In all likelihood, the errant address isn't even owned by PayPal.

Another common technique is to omit or reverse a few letters. In this way, www.amazon.com becomes www.amzaon.com or www.amzon.com. The addresses are so close that people just skimming—and not really looking for tricks—are easily fooled. You may have seen several web addresses like this without even realizing that everything wasn't kosher. Research conducted by reading specialists has found that our minds automatically fill-in missing letters and words without most readers even noticing. Like so many parts of phishing, this is another practical application of social engineering.

Clever cyber criminals are also using URL shortening services to hide behind what looks like a real link. URL shortening services have been around for quite a while. TinyURL started in 2002. Today, there are over 100 different shortening services available. A URL shortening service does exactly what it sounds like it would do. It allows the user to shorten a long URL by creating a short alias, like a nickname. When used honestly, URL shortening services are a great service to mediocre typists. When used dishonestly, shortened URLs can be used to redirect users from a seemingly respectable or trusted website to a site featuring unrelated ads, inappropriate content, or malware. Because the use of shortened URLs in Internet scams is increasing, some applications will automatically expand shortened URLs for you to let you see exactly where you're going. Desktop applications like Tweetdeck display a window that shows both the shortened and full-length URLs. The Twitter website also expands shortened URLs as you mouse-over them, even within tweets with embedded Javascript.

Even if you expand a shortened URL, it's not all that easy to tell whether the website is malicious. Some websites use domain names designed to trick users by including part (or all) of the URL of a legitimate trusted website. For example, www.facebook.com.badguy.com, is actually NOT part of Facebook although you would certainly expect it to be from the URL.

A better solution to the problem of malicious links is to actually filter out the bad links. Because so many of their users are being targeted by phishers using deceptive URLs and links to malicious websites, social networking sites are beginning to do just that. In March 2010, Twitter announced that it would automatically route all links submitted to Twitter through a service to check for malicious URLs. No doubt, the other social networking sites will follow suit, and the bad guys will look for a new way to target users.

In the meantime, you can never be entirely sure where any given URL will take you. To stay safe on the journey, make sure that your antivirus and anti-spyware protection is up to date.

7.3 Phishers of Friends

A recent phenomenon in the world of phishing has been attacks on social networking sites. Often these begin as wall postings or status updates that contain links, as well as social engineering techniques to encourage click-through. One popular scam from 2008 reported by Michael Arrington at TechCrunch consisted of wall postings in the format:

```
lol i cant believe these pics got posted.... its going to be BADDDD when her
boyfriend sees these- http://www.facebook.com.profile.php.id.371233.cn
```

Users who clicked through were taken to what looked exactly like the Facebook login screen. Obviously the goal was to collect Facebook user IDs and passwords. Why? First, it's an easy thing to do. Collect one user's sign-in and you can repost the message to all her Friends, picking up at least some of their sign-in data in the process. Then to their Friends, and so on. Once the phisher has a critical mass of Facebook IDs, he can sell them to a spammer.

In response to repeated phishing attacks in 2009, Facebook spokesman Barry Schnitt advised users to make sure their address bar read www.facebook.com before signing in. Schnitt also advised that, "People should have a healthy dose of suspicion, and ask themselves 'why did I get logged out?'"

7.4 The Disaster Con

Phishers and other scammers frequently take advantage of the human desire to help. Jennifer Perry, managing director at E-Victims, notes that, "As soon as there is a catastrophe, such as cholera in Zimbabwe or conflict in Gaza, within hours there will be scams run by criminals trying to get charity for those causes." In 2005, there were so many fraudulent websites set up scamming contributors that the FBI joined forces with the Justice Department and other groups to create the Hurricane Katrina Fraud Task Force. With the 2010 Haitian earthquake disaster, the fraud became global. Within four days of the Haiti earthquake, over 400 new Internet sites had been registered related to Haiti. While some of those were legitimate, many were created specifically to harvest credit card information from

would-be donors. Within two weeks of the disaster, Federal officials had received 170 complaints of related fundraising scams. According to Kevin Haley, director of Symantec Security Response, "Cybercrooks are also manipulating online searches so that results for terms such as 'Haiti relief fund' and 'Haiti donations' direct people to phishing sites or pages laden with malware." To avoid this particular form of phishing, experts advise skipping the search and going directly to the website of a trusted, well-established non-profit. Note the address carefully, avoiding addresses that contain mostly numbers (a common technique used by scammers). Also note that most legitimate nonprofit websites end in .org not .com.

7.5 Don't Let the Phishers Hook You

Legitimate banks and e-commerce sites never send emails requesting account numbers, passwords, social security numbers, or other personal information. The problem, however, is that the emails phishers send requesting this information look so real that many people have been tricked into giving the phishers what they are looking for.

Don't ever update or provide a bank account number, login information, social security number, IM login and password, or any other kind of personal information, no matter how official the site looks. Your parents might not be aware of this type of fraud, so educate them to make sure they don't get hooked by phishers.

Chapter 8

Safe Cyber Shopping

Meet Frank Wong, a 15-year-old cyber-shopper from Cleveland, Ohio. Frank began his online commerce experience when he used his mom Sally's credit card to open his Xbox 360 account. A few weeks later, Sally was blown away when Frank asked if he could buy his T-shirts online. The mall didn't carry the cool shirts that Frank wanted. Buying Frank's shirts online saved Sally a trip to the mall and she's been happy to have Frank purchase his own T-shirts, books, and other supplies online. Sally hates the mall.

Frank still can't remember the combination to his school locker. But he has memorized Sally's Visa number, even the expiration date and verification code! Sally's not all that thrilled about his ability to memorize her credit card information, but she loves shopping online.

This year, Sally will be far from the only mom—or dad—skipping the mall for the convenience of shopping online. **eCommerce** has become a major part of the American consumer experience.

eCommerce Electronic commerce. The business of buying and selling stuff online.

A mere decade ago, online shopping seemed the province of upscale professionals and the technological elite. No more. Today, grandmothers and programmers alike peruse Amazon and eToys for that perfect birthday gift. The ranks of eBay users have also swelled to include a substantial percentage of holiday shoppers.

At first glance, online shopping seems one of the few areas where teens aren't leading the pack in Internet usage. Internet shopping is actually highest among those people demographers call Gen X and the Millennials. Gen X includes those people born from 1965 to 1976, 80% of whom shop online. The Millennials are those people born from 1977 to 1990. 71% of them shop online. In contrast, only 38% of users under 18 shop online. Sort of. The biggest difference between teen users and their X-men or Millennial elders is actually who's holding the credit card. Teens under 18 who shop online are obviously doing so with someone else's credit card. When you factor in the number of teens who receive goods bought online which they actually picked out themselves but had a parent order, you get a much higher percentage of online shoppers.

As online shopping has taken off, the general public has also become more aware of both privacy and security issues. Sending credit card numbers and **eChecks** makes some people a bit paranoid. An eCheck is an electronic version of a bank check. Unlike a money order (which is a check-like piece of paper that anyone can buy using cash even if they don't have a checking account), an eCheck is tied to a specific bank account just like a real check. It simply exists only electronically, not on paper.

eCheck An electronic version of a bank check.

eCommerce should make people a little nervous, but within reason. Although online fraud has expanded along with eCommerce, online paranoia has expanded even faster. Should you be careful about shipping off your parents' Visa numbers

to perfect strangers? Absolutely! Is this really more dangerous than handing their credit card to another cashier at the mall? Maybe not.

Obviously, there are real dangers and risks in using those Check Out options on the Internet. But it's important to put those dangers in perspective. In this chapter, we'll examine the real risks of online commerce and talk frankly about how to minimize those dangers while taking advantage of the wonders and freedoms provided by putting the world's malls at the tip of your keyboarding fingers.

8.1 Online Shopping Basics

As reliable broadband service has become available to most American consumers, the number of online shoppers has skyrocketed. Cyber Monday is now as much a part of our holiday season as Black Friday, and gaining on its predecessor. In 2009, Cyber Monday sales topped $887 million. Amazingly, that wasn't even a record-setter for a single day's online sales. That record is currently $913 million in sales recorded on December 15, 2009. That's nearly a billion dollars in online sales on a single day!

Gender Gap

When it comes to Internet usage, there really is a gender gap—but probably not the one you'd expect. The heaviest users by far of most Internet services are older teenage girls.

Fifteen- to seventeen-year-old girls out-communicate all age groups online, with **97%** using IM versus only 87% of boys the same age. And, girls set the highest rates for seeking online information about everything from college options to religion and favorite movie stars!

Online shoppers now fall into nearly every age range and most socioeconomic groups. Obviously, the poorest shoppers account for far fewer online purchases. Of course, they also account for far fewer purchases of any kind. Surprisingly though, the highest sales came from middle-income rather than the most affluent shoppers. Price-conscious netizens are especially pleased with the experience, using Search engines and comparison shopping sites to get the most bang from their shopping buck.

The spread of faster broadband connections has also had an effect on online purchases. No longer forced to wait for detailed photos or websites to download, broadband users account for the vast majority of online purchases.

The number of online shoppers is likely to continue growing. Several studies have found that once a consumer makes a "good" online purchase, she's very likely to make more and more purchases online. And, despite concerns over online scams and identity theft, most online purchases are good. A full 80% of shoppers were satisfied with their latest online purchases. Online sales offer incredible convenience—particularly when Mother Nature doesn't. When blizzards hit the East Coast in mid-December of 2009, online sales hit $4.8 billion for a single week.

Looking for a Better Deal?

Easy comparison shopping is one of many areas where online commerce beats the socks off traditional brick and mortar establishments. To compare prices on your upcoming purchases, try one of 2009's top comparison shopping sites:

- NexTag
- PriceGrabber
- PriceRunner
- Pronto.com
- Shopping.com
- Shopzilla
- StreetPrices.com
- Yahoo Shopping

8.1.2 What Are They Buying?

Mention online buying to an average newbie and you're likely to get a comment about eBay. While the online auction giant is still the place to go for obscure teacups and collectibles of any genre, eBay no longer rules the roost in online sales. By 2010, the top markets included fixed price offerings by both eCommerce only sites and online versions of traditional chains.

So what are shoppers buying online? Almost everything:

Electronics and Computer Goods

As you might expect, electronic goods sell briskly online. After all, these are the goods specifically targeted to the most technologically savvy online users.

Clothing

When LL Bean and Lands' End began offering online shopping to traditional catalogue customers, they began a trend that still shows no signs of abating. While LL Bean and Lands' End still dominate in this market, they've now been joined by Old Navy, Gap, Hot Topic, Forever 21, Delia's, Hollister, Pac Sun, and Victoria's Secret.

Books

Sales of both new and used books have also surged online. Amazon leads the pack, but a wide variety of challengers (Barnes and Noble, Borders, Abe Books, etc.) follow with strong sales figures. Amazon, of course, sets some pretty astronomical figures to follow. Amazon media sales topped $12 billion worldwide in 2009. Although not all of those purchases were books ("media" includes books, music, and DVDs), that's still a lot of happy readers!

Almost Anything Else

For obscure items in almost any category, eBay still leads the pack. While eBay has taken on almost mythic proportions in pop culture, its real presence is still pretty impressive. During just the last quarter of 2009, over $2.04 billion dollars worth of goods were traded there. Altogether, eBay's 90 million registered users bought $2,000 worth of goods every second during 2009. Incredibly, that was a decrease from 2008, reflecting the general downturn in the economy.

eBay has also been getting some competition from craigslist, a service that offers free postings to would-be sellers and traders.

For the not-so-obscure items, let's not forget Walmart. They offer a wide range of ordinary, general merchandise online. In July 2009, Walmart.com had over thirty-two and a half million visitors.

8.2 Shopping Problems

Although 80% of online shoppers have been happy with their experiences, there are still a number of pitfalls to be navigated in the commercial corners of cyber space. The most important, to most users, are understanding (and avoiding) data pharming, and protecting yourself from both online fraud and identity theft.

8.2.1 Data Pharmers

Data pharming is one of the dangers of shopping, or even browsing, online. Simply put, a data pharmer is someone who farms the Internet, growing collections (databases) of information about Internet users.

This isn't always a bad thing. Some of the biggest names in online retailing collect a great deal of information about their buyers. These legitimate users never use

the term "data pharming." Instead, they "track preferences." Consider Amazon. If you're an Amazon buyer, chances are that Amazon knows a good bit about you and your online buying habits. They keep track of what you look at as well as what you buy. They track your purchases and even use that data to suggest other items that you'd probably be interested in. If you buy one book in a series, Amazon lets you know when the next book in that series is released.

Netflix, the online movie rental company, does the same. When you rate movies on the Netflix site, they compile your ratings and use those to recommend similar movies that you'd probably like.

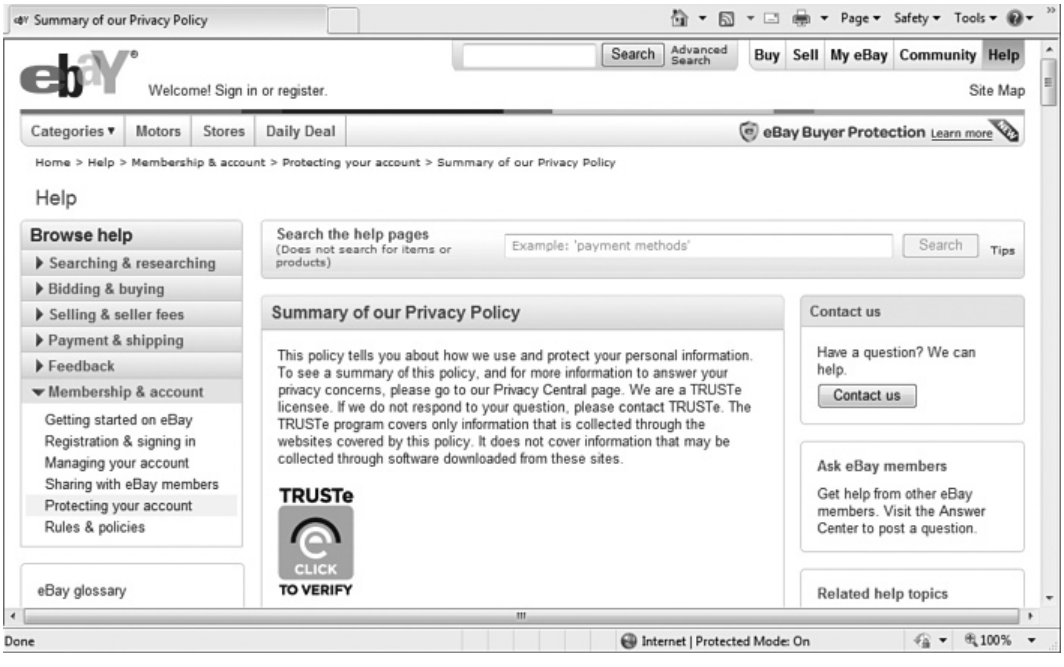
Often, this preference tracking can work to your advantage. We've found that over 75% of the movies that Netflix thought we'd love were films that we'd already seen and liked or had planned to see eventually. Likewise, we've ordered at least a handful of Amazon's suggestions and been quite pleased with the results.

Where preference tracking becomes a problem is when you aren't aware that your preferences are being tracked, or you're not told who that data is being sold to or even that it is being sold. If you are aware that your online purchases are being tracked, remember to ask yourself, "How secure are the systems that keep track of what I buy?"

Most importantly, when you're considering a purchase with a new online site, find out what kind of privacy policies they have. Legitimate sites have links from the home page (and most other pages), taking you directly to the privacy policy.

The Amazon Privacy Notice link appears at the bottom of every Amazon page

That policy will tell you whether or not they sell information about you and your purchases. Don't assume that if the Privacy Policy is front and center that your privacy is being protected. A very large number of eCommerce sites DO sell information. They get away with that because most users never bother to read the posted Privacy Policy. Don't stay in the dark about where your information is going. Always read the Privacy Policy. No privacy policy? Then there's probably no privacy either. We strongly suggest you shop elsewhere.



eBay Privacy Policy

8.2.2 Hijackers

Unlike being pharmed, which can be good or bad, being **hijacked** is always a bad thing. What a hijacker does is send you to a different site than you think you're going to. You might believe you're at eToys.com when you're really looking at a well-spoofed site and handing your parent's credit card numbers to some con artist in the Ukraine.

Hijacking Rerouting a user from the website they thought they were going to into a different (often spoofed) site without their knowledge.

Spoofing

Users can be tricked in several ways. You already know that fraudsters often spoof well-known sites by creating fake sites that look very much like the real site but exist at a different Internet address (URL). Attackers send email and post links to the spoofed site in the hopes that unsuspecting users will enter personal and financial information. We talked about this in *Chapter 7, Phishing for Dollars*. The problem is becoming more common as phishing schemes proliferate but is thankfully easy to avoid. Simply NEVER go to a site by clicking on a link provided in an unsolicited email. Instead, type the URL as you know it in the address bar of your web browser. Problem solved.

Usually. Sometimes, however, the problem isn't a phishing scheme email so much as a user with poor spelling or typing skills. They type in the URL address themselves; they just don't spell it correctly. Spoofers select URLs that reflect common misspellings of commercial website URLs. Thankfully, most Internet security packages now check for this type of re-routing as part of their standard fraud prevention. That's one more reason to make sure that you're using a quality Internet security package.

DNS Poisoning

The second way that users are hijacked is harder to avoid. It's called a **DNS poisoning**. DNS poisoning occurs when a hacker breaks into your local DNS server. The DNS server (spelled out Domain Name Service) is what translates the domain name you type into the correct numerical Internet address. You type in www.google.com and it takes you to the specific Internet address where Google

lives. This greatly simplifies using the Internet for you, since it's a lot easier to remember a named URL like www.CNN.com than it is to remember an Internet address like 192.123.0.0.

DNS poisoning Compromising a domain name server to hijack users without even their web browsers catching on.

A compromised DNS server can wreak havoc on Internet users. If your DNS server is poisoned, you could actually type in the correct URL exactly the way it should be typed and still end up on some con artist's website. Even worse, your web browser would actually believe that you were on the legitimate site. There's no easy way to tell you've been hijacked.

While DNS poisoning is thankfully much less common than spoofing or computer viruses, it does happen. One German teenager managed to reroute traffic to the German eBay site, eBay.de. According to police spokesman Frank Federau, the boy wasn't even a computer expert. He told police he'd just stumbled across a website explaining the scam and thought he'd try it out "for fun." Given that he's since been charged with computer sabotage under German law, we can only hope he's reconsidered his idea of fun.

While it's harder to protect yourself from DNS poisoning than it is to avoid clicking on spoofed email links, it is still possible. You can minimize your chances of being victimized by limiting your eCommerce dealings to those sites having a valid digital certificate. We'll explain more about certificates in the next section, but for now just remember that the certificate should match the location you were trying to get to.

8.2.3 Online Fraud

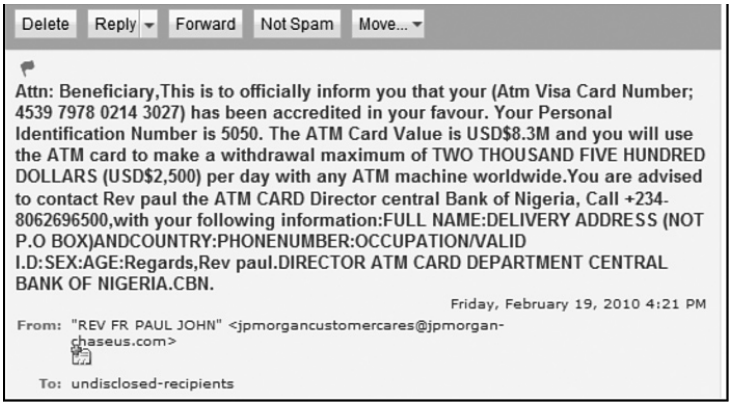
Online fraud includes purchased goods that fail to materialize, phony checks and electronic checks that never clear, work at home scams that never produce income for anyone but the scammer, and offers of "free" gifts and sweepstakes prizes which the user can claim only after paying shipping or taxes. In these cases, the prizes either never materialize or turn out to be worth substantially less than the handling fees required to collect them.

There's also a whole category of scams referred to as Nigerian money offers. This is one of the longest running scams on the Internet, having started in the 1980s, and seems destined to continue almost in perpetuity. Anyone who's used the Net more than six or eight months has received at least several of these offers. This scam is SO common that at one point, the Financial Crimes Division of the Secret Service received nearly 100 phone calls a day about it.

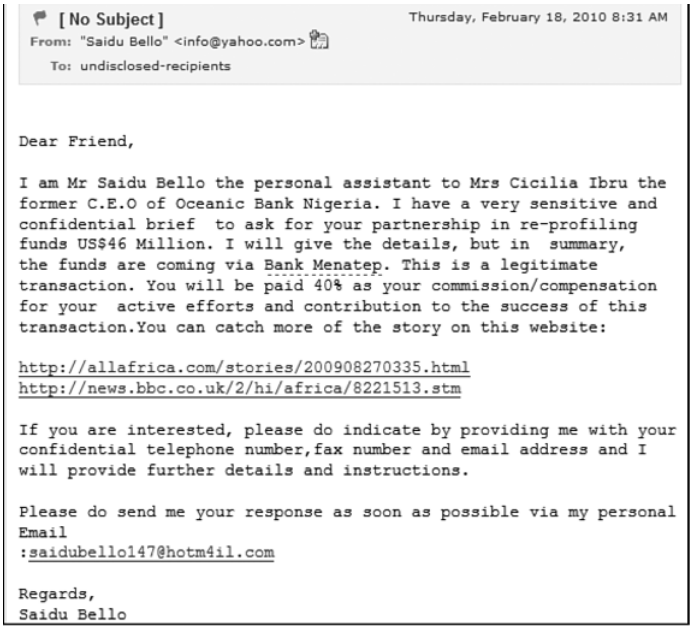
```
LAGOS, NIGERIA.
ATTENTION: THE PRESIDENT/CEO

DEAR SIR,

CONFIDENTIAL BUSINESS PROPOSAL

HAVING CONSULTED WITH MY COLLEAGUES AND BASED ON THE INFORMATION GATHERED FROM THE
NIGERIAN CHAMBERS OF COMMERCE AND INDUSTRY, I HAVE THE PRIVILEGE TO REQUEST FOR YOUR
ASSISTANCE TO TRANSFER THE SUM OF $47,500,000.00 (FORTY SEVEN MILLION, FIVE HUNDRED
THOUSAND UNITED STATES DOLLARS) INTO YOUR ACCOUNTS. THE ABOVE SUM RESULTED FROM AN
OVER-INVOICED CONTRACT, EXECUTED COMMISSIONED AND PAID FOR ABOUT FIVE YEARS (5) AGO
BY A FOREIGN CONTRACTOR. THIS ACTION WAS HOWEVER INTENTIONAL AND SINCE THEN THE FUND
HAS BEEN IN A SUSPENSE ACCOUNT AT THE CENTRAL BANK OF NIGERIA APEX BANK.

WE ARE NOW READY TO TRANSFER THE FUND OVERSEAS AND THAT IS WHERE YOU COME IN. IT IS
IMPORTANT TO INFORM YOU THAT AS CIVIL SERVANTS, WE ARE FORBIDDEN TO OPERATE A FOREIGN
ACCOUNT; THAT IS WHY WE REQUIRE YOUR ASSISTANCE. THE TOTAL SUM WILL BE SHARED AS
FOLLOWS: 70% FOR US, 25% FOR YOU AND 5% FOR LOCAL AND INTERNATIONAL EXPENSES INCIDENT
TO THE TRANSFER.

THE TRANSFER IS RISK FREE ON BOTH SIDES. I AM AN ACCOUNTANT WITH THE NIGERIAN
NATIONAL PETROLEUM CORPORATION (NNPC). IF YOU FIND THIS PROPOSAL ACCEPTABLE, WE SHALL
REQUIRE THE FOLLOWING DOCUMENTS:

(A) YOUR BANKER'S NAME, TELEPHONE, ACCOUNT AND FAX NUMBERS.
(B) YOUR PRIVATE TELEPHONE AND FAX NUMBERS -- FOR CONFIDENTIALITY AND EASY
COMMUNICATION.
(C) YOUR LETTER-HEADED PAPER STAMPED AND SIGNED.

ALTERNATIVELY WE WILL FURNISH YOU WITH THE TEXT OF WHAT TO TYPE INTO YOUR LETTER-
HEADED PAPER, ALONG WITH A BREAKDOWN EXPLAINING, COMPREHENSIVELY WHAT WE REQUIRE OF
YOU. THE BUSINESS WILL TAKE US THIRTY (30) WORKING DAYS TO ACCOMPLISH.

PLEASE REPLY URGENTLY.
BEST REGARDS
```

Traditional Nigerian Money Offer

Because this scam is so pervasive, there are probably several hundred variations on the theme. Some scammers throw everything into the subject, assuming that you're not likely to read the message body.

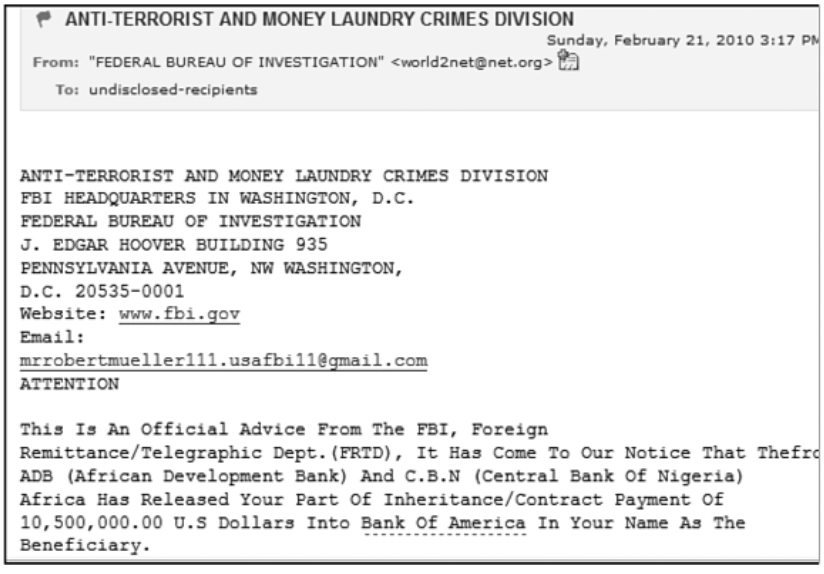


Others begin with the money scam approach, but are really angling to load your computer with malware by piquing your curiosity enough that you forget common sense and click on links embedded in the email for "more information."



A few even acknowledge how well-known the scam is before launching into it. This is a great social engineering approach. The crook is basically saying, "Poor me. Wouldn't it be awful to be a legitimate businessman in a country that's known mostly for its online criminals?"

Still, our favorite would have to be the Nigerian scam that's spoofed to appear as if it came from the FBI.



ANTI-TERRORIST AND MONEY LAUNDRY CRIMES DIVISION

Sunday, February 21, 2010 3:17 PM

From: "FEDERAL BUREAU OF INVESTIGATION" <world2net@net.org>

To: undisclosed-recipients

ANTI-TERRORIST AND MONEY LAUNDRY CRIMES DIVISION
FBI HEADQUARTERS IN WASHINGTON, D.C.
FEDERAL BUREAU OF INVESTIGATION
J. EDGAR HOOVER BUILDING 935
PENNSYLVANIA AVENUE, NW WASHINGTON,
D.C. 20535-0001
Website: www.fbi.gov
Email:
mrrobertmueller111.usafbi11@gmail.com
ATTENTION

This Is An Official Advice From The FBI, Foreign
Remittance/Telegraphic Dept.(FRTD), It Has Come To Our Notice That Thefrc
ADB (African Development Bank) And C.B.N (Central Bank Of Nigeria)
Africa Has Released Your Part Of Inheritance/Contract Payment Of
10,500,000.00 U.S Dollars Into Bank Of America In Your Name As The
Beneficiary.

One of the best ways to keep your online purchasing experience pleasant is to limit your purchases to reputable sellers. Like many security measures, this is, of course, easier said than done. An easy first step, however, is to avoid buying anything from spammers. Nearly a quarter (24%) of Internet scams begin with unsolicited email.

Before you bite on one of those too-good-to-be-true email offers, you might want to consider the advice of Bob Kruger, a vice president at BSA. He notes, "There are a lot of cyber-grinches out there who are only too happy to take consumers' money and spoil their holiday shopping season."

8.3 Ensuring Safe Shopping

While computer fraud has advanced in recent years, so has the technology that can help to protect the integrity of your online communications and financial transactions. Three of these technologies are especially important: encryption, authentication (SSL, digital signatures, digital certificates), and security tokens.

8.3.1 Encryption

Encryption is a technique used to scramble content in files that you don't want anyone to be able to read. This protection is critical to safe online shopping. When you shop, you're sending a LOT of information that you really don't want to share with the general public. Your credit card numbers. All your personal information—your full name, address, phone number(s), and email address(es). Encryption of one or more forms is crucial to protecting all that shopping information.

When you encrypt a file, you're applying a "code" to it so that anyone who doesn't know the code can't read the file. Unscrambling an encrypted file so that it's readable again is called decrypting it.

You can think of **encryption** as applying a type of secret code. Remember the codes you used to have to break for math class to learn logic? "Decode the secret message if A=1, B=2, C=3, etc"? This is exactly like that.

Encryption Applying a secret code (cipher) to your messages or files to keep other people from reading them without your permission.

Let's use a simple code as an example. Let's say that we're going to encrypt a message by replacing every letter with the letter that precedes it in the alphabet. Every B becomes an A, every C becomes a B, etc. When you get to the beginning, you wrap around so that every A becomes a Z. Using this code, let's encrypt the following phrase:

```
This sentence is none of your business.
```

Once we apply our "cipher" (the alphabet precedence algorithm), this becomes:

```
Sghr rdmsdmbd hr mnmd ne xntq atrhmdrr.
```

In computer terms, the first sentence, the one you can clearly understand, is called **plaintext**. This is your text, plain as day, just the way you entered it from your keyboard. The scrambled sentence at the bottom is called the ciphertext. That's your text once the encryption cipher (sometimes called the cryptographic algorithm) has been applied. If you don't know the cipher being applied, it's very difficult to figure out what the second sentence means. So, it's extremely hard to decrypt the ciphertext.

Plaintext The plain, clearly readable, text message *before* encryption.

Of course, computer ciphers are an awful lot more complicated than our sample code. Most use at least a 64-bit encryption (often 128-bit). That means that the cipher key (that's a type of password that determines the cryptographic algorithm applied to encrypt your text) has at least 64 digits—possibly many more—that need to be puzzled out in the correct sequence for a code breaker to have any hope of decrypting your message without your permission.

In Internet security terms though, even 64-bit encryption is considered pretty simple—in fact, almost lame. Larger keys are used to produce stronger encryption. In general terms, encryption strength is measured by the encryption algorithm and the size of the key. A bigger key usually means stronger encryption.

Cryptoanalysis Trying to break an encrypted message.

In addition to encryption key size, encryption methods also vary. Today, there are two major methods used to encrypt communications over the Internet: symmetric encryption and public key encryption. Symmetric encryption, also called secret key encryption, uses the same key to encrypt and decrypt the message. In symmetric encryption, both the sender and the receiver have to have the same key. Therefore, the key must be kept secret. Public key encryption uses two keys: a public key and a private key. You can use either key to encrypt the message but only one of the keys will decrypt the message.

Ciphertext A message or file after it's been encrypted. Ciphertext appears garbled and can't be read until it's decrypted.

What all of these methods have in common is that you MUST have the cipher or key to translate the ciphertext back into plain text that makes sense. No key, no content.

As you might imagine, cryptography and the art of computer encryption is pretty complicated as well as just being pretty cool. If you'd like to learn more about this topic, we suggest you start by reading *Applied Cryptography* by Bruce Schneier.

8.3.2 Secure Socket Layer (SSL)

SSL is an important layer of security if you are providing personal information such as in a credit card transaction. SSL is a protocol that encrypts the transmission of data via HTTP. You can tell if you are protected by SSL if the browser

Common Codes and Dead Cows

Ciphers—secret codes—are pretty common on the Net. IM speak (R u hm for Are you home?) is one example of a common online cipher.

Another popular code is called 1337 (and pronounced "leet"), named for the 1337 (numerical) port used for an infamous computer attack by the hacker group that calls itself the Cult of the Dead Cow.

In 1337, words are spelled using numbers and symbols to replace the letters that they physically resemble. A simple example would be:

```
31337 h4x0rz un j00! > Elite hackers own you!
```

Fluent 1337 sp33k3rz get even more obscure, replacing R's with "/2", etc. and making some pretty wild substitutes for other letters such as M, N, and W:

```
_|00 |2 4/\/ (_)83|2 |-|4><0|2! > You are an uber hacker!
```

Also note that while many 1337 comments are insults (something about the gaming culture?), you can also use 1337 to send hugs and kisses, ><><><()()()><><><><()()(), and love, <3 !

address bar displays an "https" instead of "http", and if you see the lock symbol on the bottom right of your Web browser status bar.

8.3.3 Digital Signatures, Certificates, and Hashing

While encryption protects the contents of your message, it does nothing to prove or verify that you're the person who actually sent it. This process of proving the source of a message or website is called **authentication**.

When you're shopping online, authentication is a pretty important concept. Before you hand over your parents' credit cards numbers to iTunes to download your favorite group's latest album, you want to make sure that it really is iTunes that you're talking to. In that case, while you still want and need to have those credit card numbers encrypted, you also want and need to authenticate the recipient.

Authentication Verifying the identity of a message sender or website.

Who Provides What?

Legitimate retailers know you're concerned about potential fraud. So, they provide things like digital signatures and certificates to prove to you that they're who they say they are. You just make note of what the vendor is doing to protect your data. You don't actually have to DO anything.

Three common methods are used for authentication: hashing, digital signatures, and digital certificates.

Hashing

Hashing, most commonly a one-way hash, is a method used to verify data rather than encrypt it. With this method, a one-way hash algorithm is applied to the plaintext. The result is a "message digest" attached to the original plaintext message. This digest functions as a unique, identifiable "fingerprint" for the message. If the message is changed in any way, applying the one-way algorithm will generate a "fingerprint" that no longer matches the attached digest. This process allows the message recipient to check the plaintext message received against the message digest to ensure that the file was not tampered with.

Digital Signatures

A digital signature is another method used to verify the sender of a message. Unlike hashing, digital signatures do use encryption—specifically, a type of public key encryption which uses two algorithms, one for encrypting and the other for decrypting the digital signature.

In simple terms, a digital signature is attached to encrypted data to ensure two things: (1) that the message is authentic and intact and (2) to authenticate the message sender. Using a digital signature has the same effect as using hashing along with encryption. It simply does so using a slightly different methodology.

Digital Certificates

A digital certificate takes the digital signature concept to a higher and much more secure level, by adding a trusted third party. When you buy something over the Internet, for example from Amazon.com, you are using public key infrastructure. The problem with using only public key encryption in this case is that anyone can create a public/private key pair. It's a bit complicated, but the basic idea is that it is possible to "forge" a digital signature. The signature itself would still match (the public/private key combination would still work), but the signature author might not be who you thought it was.

To avoid the problem of forged digital signatures, eCommerce retailers instead make use of a digital certificate. A digital certificate contains a person's or corporation's public key. This is exactly like a digital signature. The difference is that a digital certificate is issued by a trusted third party who verifies independently that the certificate belongs to the person claiming ownership.

You can think of a digital certificate as being analogous to a driver's license. When you obtain a driver's license, you have to provide reasonable identification to the Department of Motor Vehicles (DMV). The companies that issue digital certificates, like VeriSign, function as the DMV and obtain that reasonable identification. VeriSign's certification authority (CA) then issues a public/private key pair (for a small fee), keeps the matching public key in a database, issues a digital certificate, and keeps a copy of the certificate in its database.

8.3.4 Security Tokens

Encryption protects the contents of your messages and files. Hashing, digital signatures, and digital certificates authenticate the people and places that you're doing business with. **Security tokens** authenticate YOU.

You're probably thinking, "But I do that myself when I enter my private password." True. The problem is that passwords can be easily cracked and stolen by hackers. Security tokens provide a much stronger two-factor authentication that includes both data (often a password) and a physical device.

Two-factor authentication is something that you already use all the time offline. When you use an ATM card to withdraw money from your bank account, you're using two-factor authentication. The physical ATM card identifies you (factor one), as does the PIN number that you enter (factor two). While it's important that you don't misplace either, neither is really useful without the other. A criminal can play with your ATM card all day, but he's not getting money from your bank unless he also knows your PIN number.

Security token A two-factor authentication method using a physical device as well as a secret code.

An ATM card is only one example of a security token. Other forms of security tokens are physical tokens (a small hardware device), smart cards, and biometric systems. With biometrics, the physical component is biological data like a fingerprint or retinal scan.

Chapter 9

Browsers Bite Back

Mike spent a lot of time surfing PC gaming sites on the Internet. Still, he was a little put back one day when visiting an old gaming site he hadn't been to in five or six months. Just connecting to the site, without logging in or providing any information, he was greeted as a welcomed old friend:

```
Welcome Back Mike of Bendersville!
```

While the goal was to bring Mike figuratively back into the fold, the effect was to actually creep him out. Mike wanted to know exactly how the gaming site knew **who** he was. He began to wonder if he'd fallen victim to that spyware he'd been hearing so much about...

While it's possible that Mike had fallen victim to spyware, the link to those details that creeped him out was probably stored on his own computer, sitting in plain sight in his Cookies folder. Allowing cookies to track your activities is only one of several ways that your Internet browser can bite back.

In this chapter, you'll learn what it is that cookies do and how to rein them in to ensure that they only work FOR you and not against you. You'll also learn about browser options and how you can set them to increase your safety and security.

9.1 Making Cookies Work FOR You

Contrary to popular belief, a cookie is not a program. It doesn't DO anything per se. It's simply information passed to your web browser when you visit a website that uniquely identifies you and your system. Cookies land on your computer almost continuously as you surf the Internet. Those **cookies** are then passed back to websites every time you re-visit them. Websites use your cookies to recall information about your previous visits, to determine if you are currently logged into the site, to change some aspect of the site, to provide additional functionality for the site, or to record detailed data about your visit. Accepting cookies is part and parcel of using most websites. Some websites will not work correctly if you do not accept the cookies they provide.

Cookie Information written to your hard drive by a website that you visit. A website can use a cookie to recognize you, and sometimes remember custom settings, when you visit that site again in the future.

In general terms, a cookie is a small piece of information that consists of a single item—a name/value pair. In most cases, the "name" is a conglomeration of the website name and the user ID you've selected (or been assigned) for the site you're visiting. The "value" is a unique numeric value that the site has assigned to that name. Together, the name/value pair uniquely identifies you every time that you visit that website from the same computer.

```
NSC_mc_xxx-nbjo_80441327223660us.myspace.com/153637783381763004734420362481763004734*
```

Contents of MySpace cookie

As you can see, cookies aren't very informational to look at. They are, however, a very important thing to know about.

One common misconception about the Internet today is that when you visit a website, your web browser is only communicating with one website or one computer. That's not always true. In most cases, there are multiple websites and computers involved, each providing a small part of the web page that you see. This means that cookies can be loaded from or shared with many other websites just by loading a single web page.

9.1.1 Are Cookies Good for Me?

Sometimes, cookies allow a website to ***remember*** your customizations. Otherwise, you'd need to "customize" each site every time that you visited. That would hardly be convenient. Cookies also allow you to set convenient options, like one-click shopping and checkout on commercial sites. And they allow sites to "remember you" so that you don't need to enter your user name and password every time you visit.

But like wizards, not all cookies are good. Cookies also allow the websites you visit to keep track of you. They can record how often you visit, and which pages you use on their sites. The potential for "Big Brother" style oversight by cookies and their evil cousins, web bugs, makes a lot of web users very uncomfortable.

In general, whether you need to worry about a cookie depends on whether it's a primary cookie or a third-party cookie.

Primary Cookies

A primary cookie, sometimes called a first-party cookie, is one that is planted on your computer by the website you went to visit. If you've visited MySpace.com and ended up with a MySpace cookie on your hard drive, MySpace is the primary website. That's hardly surprising. Often, you want and/or need the primary site to store a cookie to allow you to best use that site.

Third-Party Cookies

Third-party cookies are placed on your machine from a website you never visited, at least not that you knew about. We talked earlier about web bugs, also called web beacons and transparent GIFs. A web bug is a graphic too small for you to see that's included on a web page. When you visit that web page, the "invisible" graphic is downloaded from a different web page. That "different" web page is called a third-party site because it's not the primary (1st party) site that you visited, and it's not you (the 2nd party). That makes it 3rd party.

Third-party cookie A cookie placed on your machine from a website you DIDN'T actually visit.

Technically, viewing a web page that contains a web bug downloading from a third-party site has the same effect as loading that third-party web page into your browser. Any cookies that would be sent by that third-party site also land on your computer. Using these invisible graphics, advertisers and **data pharmers** (people who "farm" the Internet for information about its users) can place cookies on your computer without you ever realizing that you've visited their websites. When those third-party cookies are linked to web bugs sent via email, the pharmers can match your email address up with any details stored on the cookie. Scan enough cookies, add the email address, and it's not long before the data pharmers can actually identify YOU, not just the cookie.

Data pharmer Someone who "farms" the Internet, growing collections (databases) of information about Internet users.

9.1.2 What If I Don't Want to Share?

If you're concerned about the cookies you may have accumulated on your hard drive, you can always remove them. Doing so will help to keep advertisers from tracking you. For many web users, that's a comforting thought. Of course, if you delete your cookies you may need to re-customize many of the websites you visit.

Usually, cookies don't include personally identifying information about you. However, that doesn't mean that the company that placed the cookies hasn't started a

database file on you that does contain personal information. Since they know your cookie and use it to identify you when you visit their site, they could easily store that cookie along with that database data. Thus, cookies can be, and often are, used in data pharming operations to collect pretty detailed information about you, who you are, and what you do online.

When you visit a site online, the **Privacy policy** of that website should tell you how and if that site collects and shares information about you. Unfortunately, most people don't take the time to read these policies.

Privacy policy The official policy of a commercial website telling you what (if any) information it collects about you and what it does with that information.

There are some simple steps you can take to control how cookies can be set on your PC. In theory, you can even block cookies altogether. If you do block all cookies, you may find that you're unable to use many pages on the Internet. For example, if you choose to block all cookies, your Yahoo! mail account simply won't work.

Remember also, that many cookies are good. They provide added richness and utility to the websites you use most often. So, you really don't want to block all cookies and certainly not all first-party cookies. The trick is to find a happy medium.

9.1.3 Clearing the Crumbs

Like real cookies are good for the taste buds but usually bad for the hips, electronic cookies can also be both good and bad. At first glance, it's hard to see a bad side to an electronic shortcut that allows you to customize your web surfing experience with minimal effort. In their best light, cookies save you time and make your web surfing more comfortable, convenient, and efficient.

At the same time, however, cookies are a threat because they collect information about what you do online. Like any information collected without your explicit consent, they represent a threat to your privacy.

Cookies can also represent a threat to your identity and your personal information. While cookies themselves don't store passwords or personal information, they identify your computer to websites on which you may very well have entered identifying information. Using cookies associated with web bugs, savvy data pharmers can glue the pieces together—email address, personal information entered online, web surfing habits. The cookie itself may not contain any sensitive data, but it's the map that links the pieces together for the data pharmer.

9.2 Choosing Your Browser

If you're looking for a clear recommendation on which browser is safest to use, you're definitely looking in the wrong place. The truth is that there are advantages and disadvantages to all the major browsers.

For most people, selecting a browser really isn't an issue. They use whatever came with their computer and never give it a second thought. Obviously, the top browser at any given time is whatever is shipping preloaded on new computers. Right now, that would be Internet Explorer for Windows machines. Some people don't even realize there are other options.

Even when people do realize there are options, any web browser that needs to be downloaded and installed is at a distinct disadvantage. That includes the major alternatives, like Firefox, as well as lesser-known browsers like Google Chrome, Opera, OmniWeb, and Safari for Windows.

If you're happy with what you've got, or even just unwilling to spend the time to learn how to use a new browser, you should know that you're in the majority. Feel free to skip on to the next section with a clear conscience.

If you're not happy with your current browser, that's OK too. While Internet Explorer users are in the majority, a minority of users prefer Firefox. Firefox is a free web browser produced by the Mozilla Corporation. It is an alternative to the web browsers included with operating systems, such as Windows Internet Explorer

or Mac OS X Safari. Firefox is the second most popular web browser (after Internet Explorer). There are also other independent web browsers like Opera and Google Chrome.

Regardless of which browser you ultimately select, be aware that you still need to apply browser updates regularly to make sure that any security holes that appear are plugged quickly.

9.3 Opting for Internet Explorer

Whenever you get a new PC, in addition to installing antivirus software and applying patches, you need to select your privacy settings. Ideally, you should do all of this before you begin using your new computer online. If you opt to use Internet Explorer 8 as your web browser, you should also take the time to consider the browser options you want to set.

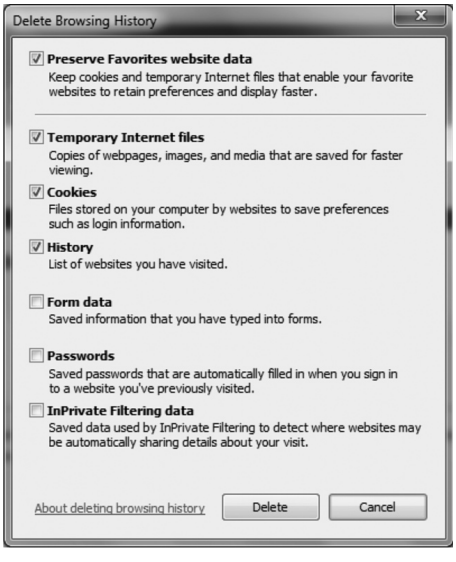
9.3.1 Clearing Address Bar Lists

Many website addresses (URLs) are long, obtuse, and difficult to type. On your own computer, it's nice to have Internet Explorer remember where you've been. Type in the first few letters and Internet Explorer can fill in the rest.

On a public or shared computer, you may not want to leave a record of every site you've visited. Even on a shared family computer, you may not necessarily want a complete list. To instruct Internet Explorer not to remember all those sites, go to **Tools > Internet Options > General**. You can ask Internet Explorer to delete your browsing history automatically when you exit the browser.

9.3.2 Clearing Temporary Files, Internet History, and Cookies

While you can always delete your browsing history on exit, you can also delete ALL the temporary files created about you in one fell swoop. Simply click on **Safety > Delete browsing history**. You'll be given easy options to clear out a lot more than just your address bar:

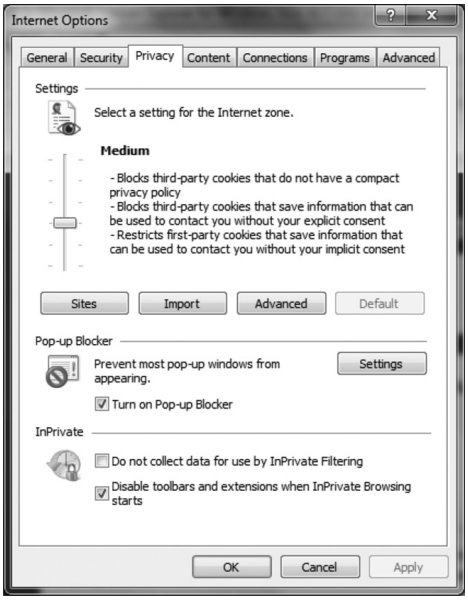


This is a great option to use because temporary files are created when you visit sites and even download images. Over time, the directory that stores temporary Internet files can take up a lot of unnecessary storage. It can also provide a clear picture of where you've been online—just as clear as looking at your browser history. By default, Internet Explorer keeps this temporary information around for 20 days. This option lets you speed up the deletion process.

One of the nicer features added in Internet Explorer 8 is that you can now throw away temporary files but KEEP your Favorites. This allows you to dump the junk without having to once again tell the TV Guide website whether you have cable or satellite, or informing your favorite Weather website where you live by inputting your zip code again. This feature can also throw away form data you entered online, but keep the passwords to your favorite sites that you've asked Internet Explorer to remember. Overall, this provides a very nice balance between convenience and security. In the long run, that's really what we're all looking for.

9.3.3 Setting Your Cookie Policy

While you're throwing away temp files and clearing your browsing history, you might as well tailor your cookie policy. To see what your current policy is, click on **Tools > Internet Options > Privacy.**



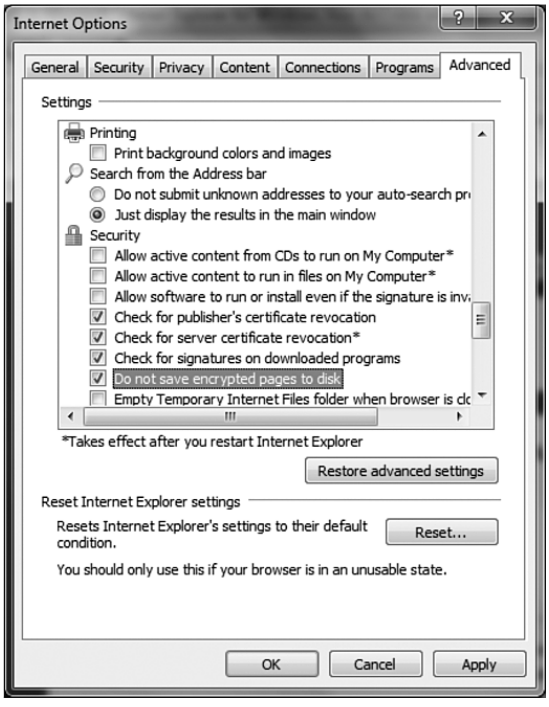
By default, your privacy is set to **Medium**. If you'd like to adjust that to explicitly block third-party cookies while allowing first-party cookies, click the **Advanced** button.

9.3.4 Storing Sensitive Data

Sometimes, like when you're shopping online, you have to protect the data that you're sending over the Internet. To safely send that data, you need to use a secure connection. In a secure connection, your data is encrypted while it travels over the Internet. Thus, credit card numbers, account numbers, and other sensitive data are encoded so that they can't be read by anyone except the website to which you're sending them.

If you read ***Chapter 8, Safe Cyber Shopping***, you already know about encryption. You may even have guessed that the encrypted data is decrypted as it arrives so that your browser can display it. What you probably didn't guess is some decrypted data is saved in your temporary Internet files. That means that if you download malware to the machine that your mom uses for online banking, that malware could potentially access your mom's bank account details by scanning the temporary files. This is also one of several reasons why you should be very wary of accessing secure financial sites from public computers at Internet cafes.

To remove the risk of having confidential data lying around in your temporary files, you'll want to instruct Internet Explorer not to save encrypted pages. To do so, click **Tools > Internet Options > Advanced**. The list of options is pretty long, so you'll need to scroll down to the **Security** section to check the box next to **Do not save encrypted pages to disk**.



9.3.5 Using InPrivate Browsing and Filtering

Most of the settings we've looked at so far involve asking Internet Explorer to delete information it's been keeping about you. The InPrivate functions are about asking Internet Explorer to not keep that information in the first place. To ask Internet Explorer not to accept cookies, record browser history, or create temporary Internet files, click **Safety > InPrivate browsing**.

9.3.6 Performing Anti-Phishing Checks

Phishing filters in Internet Explorer 8 help you to avoid online fraud. When you turn on the SmartScreen filter, Internet Explorer checks links against a database of known phishing and malware sites. Most importantly, it performs this check *before* accessing the sites.

To turn on the SmartScreen filter in Internet Explorer, click **Safety > SmartScreen Filter > Turn On SmartScreen Filter.**

9.4 Opting for Firefox

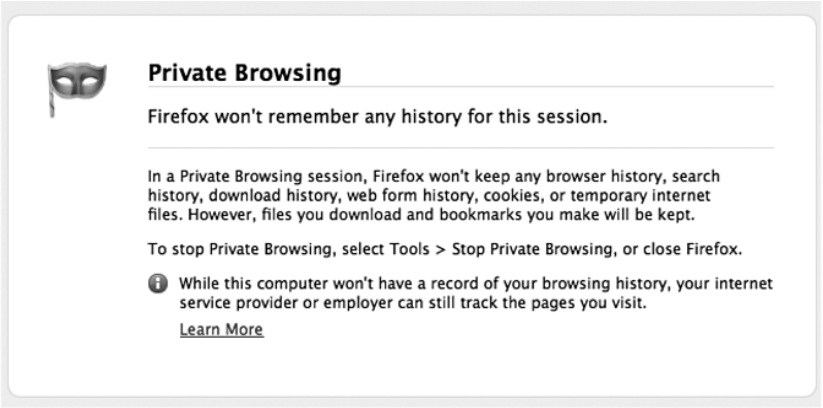
The Mozilla Corporation distributes Firefox for free from its website (getfirefox.com). Not only is Firefox free, but its source code is freely available as well. That's a big deal for programmers and aspiring programmers.

Because the source code is freely available, some programmers like Firefox. Not only can you look at the code to see exactly what it's doing, you can even add your own functions. If you choose, you can share those functions with other users. Functions like that, which are "added on" to the core browser, are called add-ons. Quite a number of add-ons are available for Firefox. Some of these add-ons provide minor tweaks to the way Firefox works (like adding "Restart Firefox" to the start menu). Other add-ons provide full-blown application functionality, including entire sets of web developer tools.

Another advantage of Firefox is that it runs on all the major operating systems. That includes Windows, Mac OS X, and Linux. There's even a version currently being developed that will run on mobile devices like smart phones. Firefox is also fast and getting faster. So far, every release of Firefox improves performance.

Firefox has a number of standard security setting features. In Firefox, you can:

- Block pop-up windows (which are usually ads)
- Browse anonymously (Firefox calls this setting "Private Browsing"; Internet Explorer calls it "InPrivate." To enable Private Browsing, select **Tools > Start Private Browsing**.)
- Set a cookie policy (banishing third-party cookies if you like)
- Clear all your temporary files when the browser exits
- Perform anti-phishing checks, having your browser check websites against a database of known phishing sites
- Run checks for updates to the core browser software and add-ons you've installed.



Firefox also provides additional functions to improve your browsing experience.

9.4.1 Detecting Outdated Plug-ins

Older plug-ins may have software vulnerabilities that put your computer and your data at risk. While browser updates are automatic, it's often difficult to tell when a plug-in has become outdated. Mozilla currently provides a webpage that tracks the current (new) versions of the major Firefox plug-ins. Plans are also underway to automate this feature for future versions of Firefox.

9.4.2 Disabling Advanced JavaScript Options

JavaScript is a simple object-oriented programming language that website developers use to jazz up their websites. Because it's easy to use, JavaScript is used

Add or Plug?

Wondering about the difference between an add-on and a plug-in?

Both items let your browser do things it couldn't accomplish on its own. The difference is that a plug-in is a complete program on its own.

An add-on isn't. The add-on "adds" functionality to the browser, but it won't work on its own in a different environment.

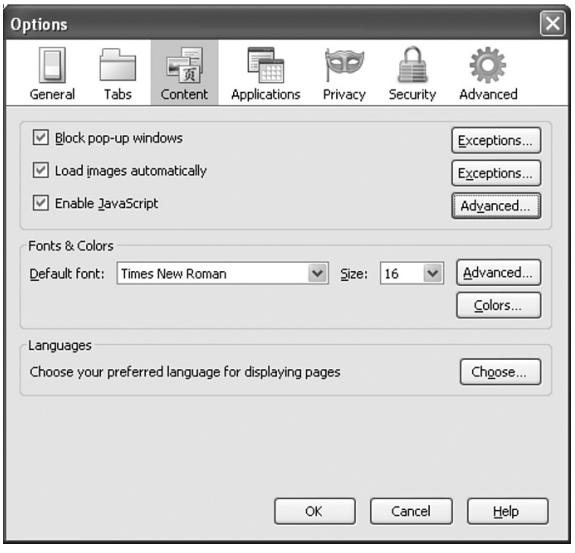
A plug-in (like Flash) works on its own OR with the browser. For example, Adobe Flash allows you to view animation in video games offline as well as on websites using your browser. That's why it's a plug-in and not an add-on.

extensively to provide sophisticated audio, video, and visual effects. Unfortunately, JavaScript has a number of security issues. While most are merely annoying, others provide the potential for unscrupulous developers to use JavaScript deficiencies to steal your sensitive information.

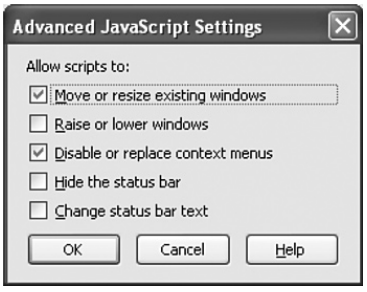
By default, Firefox enables JavaScript, even supporting most of its advanced features. In theory, you can configure Firefox to disable JavaScript altogether. Like disabling all cookies, that's not a practical solution. JavaScript has become a key website technology. Turning it off completely will make the web less fun and interesting.

Luckily, you can prevent some JavaScript security issues by disabling just the advanced JavaScript features. To disable the advanced JavaScript features, do the following:

1. Select **Tools > Options** from the Firefox menu.
2. Click on the **Content** tab of the dialog box that appears.



3. By default, **Enable JavaScript** will be checked. Leave that checked, but click the **Advanced** button to the right. A dialog box will display showing the advanced JavaScript options.



4. Uncheck all of these options.

While disabling these features solves many of the security problems inherent to JavaScript, an even better solution to manage JavaScript safely is to use the NoScript add-on described in ***Section 9.4.5, Firefox Add-ons That Make Life Easier.***

9.4.3 Disabling Java

You're probably thinking: Java and JavaScript must be the same thing, right? You would think so, but no. Java was invented by Sun Microsystems before JavaScript was invented by Netscape.

Sun Microsystems? Netscape? Never heard of them? That's not surprising since neither company exists anymore. In their day, however, both were major players in the development of Internet applications. Java continues to be a major player. While JavaScript was originally designed for use in the web browser, Java is general-purpose system that has been integrated into web browsers. That is, it's a technology designed to allow web designers and similar users to easily add interesting functions and features to their websites.

Java is a very versatile technology. It can be used to run large desktop applications like OpenOffice (a free office productivity suite) or small web-based tools (called "applets").

Java can also be exploited by malware writers. To limit that danger, Java applets have restrictions placed on them. Applets cannot access the files on your system or make network connections to any system. Still, your operating system will occasionally ask you about a Java applet that is asking for additional access. In general, unless you're absolutely sure of what the applet's trying to do and why, you should

tell it no. You should also make sure that you're using the latest version of Java and that any updates have been applied to remove potential security holes. Although the company that first produced Java no longer exists, this product is now maintained by Oracle. Visit Oracle (www.oracle.com) for update information.

9.4.4 Using a Master Password

A major stumbling block to security for many users is creating—and remembering—strong passwords. Because strong passwords are hard to guess, they are also hard to remember. For that reason, many people who set a good strong password will use that same password over and over again on multiple sites. The problem is that if attackers get access to your password by compromising one website you use, they may use that password to get access to your other accounts.

Firefox solves the memory issue by storing user names and passwords for you automatically and retrieving them as you need them. Even better, you can set a master password that then protects all the saved passwords.

To set a master password, do the following:

1. Select **Tools > Options** from the Firefox menu.
2. Click on the **Security** tab of the dialog box that appears.

3. Check the box next to **Use a master password.**

4. Enter a strong password. Since this will now be the ONLY password you need to remember, you have no excuse for not making this an outstanding password choice. Try to extend the bar as far as possible on the displayed **Password quality meter.**

Note that from the **Security** tab you can click **Saved Passwords** to display a list of the saved passwords and associated user names. (Actually, the user name listing is a great feature. People often forget user names as well passwords for sites they don't use often.)

9.4.5 Firefox Add-ons That Make Life Easier

In addition to the built-in features, Firefox can be extended by downloading and installing a number of add-ons that provide even more functionality.

NoScript

NoScript is an add-on that can disable JavaScript on web pages, put limits on the types of JavaScript permitted, and block known attacks. As you learned earlier, you can simply use Firefox Tools to disable advanced JavaScript. The downside is that setting those options is an all-or-nothing deal. The advanced features are either always allowed or always prohibited. NoScript lets you allow JavaScript on websites that you trust and block JavaScript on all other websites. That puts the power in your hands. You just need to be careful not to trust too many sites; otherwise, this add-on won't provide much protection.

Better Privacy

Adobe Flash is a multimedia plug-in used by a lot of websites to provide animation, video, and various interactive functions. What many users don't realize is that the Flash Player plug-in stores cookies (just like browser cookies) that could allow some sites using Flash to keep track of you. Unlike traditional browser cookies, these cookies can't be managed or deleted by changing your web browser settings. Better Privacy is an add-on that manages those Flash cookies. You can use this add-on to allow only specific cookies to be saved, and to delete Flash cookies periodically, or automatically when you exit Firefox.

CookieSafe

CookieSafe is an add-on for managing traditional cookies. You can control cookies for individual sites by blocking them permanently, allowing them temporarily or for the session, or allowing them permanently, all from the status bar icon for CookieSafe. This add-on also maintains a list of "un"trusted sites and blocks all cookies from those sites. Using CookieSafe, you can also share your allowed cookies and sites settings with Firefox browsers on other computers.

WOT—Safe Browsing Tool

The Web of Trust ("WOT") add-on is a collaborative web trust system that allows users like you to report back on which websites are really trustworthy. With WOT,

you rate your level of trust in a website in a variety of categories, such as trustworthiness, vendor reliability, privacy, and child safety. The WOT plug-in combines your ratings with those of other users. A "traffic light" indicator provides a dashboard view of the overall level of trust.

Password Hasher

How many web passwords do you have? Hopefully you have a unique and difficult password for every site you visit. (We hear you laughing.) Password hasher solves this problem by allowing you to create a single password that is used to create strong and unique passwords for every site you visit. The individual passwords are then stored in an encrypted Firefox password database.

9.5 Opting for Google Chrome

Released in 2008, Google Chrome is one of the newer browsers. It includes support for all of the major standards for web browsers and web page layout and scripting.

How it will fare against the established heavyweights in this market (Internet Explorer and Firefox) remains to be seen. The browser market is notoriously hard to break into. Having said that, Google does have the advantage of serious name recognition. They also have a primo advertising spot for Google Chrome, on one of the world's most popular search engines.

Google also took an interesting approach to developing the Chrome browser. Instead of building the entire web browser from scratch, Google used some of the best software already available. They used many of the open source libraries used to build other browsers, like Firefox and Safari. This allowed them to select libraries with excellent performance (speed). In some cases, Google also developed their own libraries. They have released many of these libraries and a portion of the Google Chrome source code as open source. Other companies or individuals may build their own web browsers using this code as well.

Google addresses security issues in several ways. Periodically, Google Chrome downloads a list of known websites for malware and phishing, and it will warn you if you attempt to go to one of these sites. In addition, Google Chrome protects

your information by isolating many functions from each other. This isolation technique prevents data you access using one function from being accessed by another function. This in turn reduces the opportunities for malware to access your data. Google Chrome uses a similar isolation technique to deal with vulnerabilities in web browser plug-ins, like Adobe's Flash Player.

Like Internet Explorer and Firefox, Google Chrome supports private browsing. What Internet Explorer calls InPrivate and Firefox calls Private Browsing, Google Chrome refers to as Incognito.

It remains to be seen if Google Chrome will become a dominant web browser. For the most part, the web browser wars were won years ago. However, new entrants rarely have as weighty a proponent as Google. Even if Google Chrome quickly goes the way of Netscape and Mosaic (earlier browsers that you've probably never even heard of), we can be sure that Chrome's new security techniques and certainly its open source libraries will be incorporated into other web browsers. So, you'll no doubt be seeing the legacy of Google Chrome even if you never see the actual browser.

9.6 Understanding the Plug-in Predicament

We've talked about a number of plug-ins in this chapter. A **plug-in** is a piece of software that adds functionality to another software program. Many plug-ins are available for web browsers and Internet applications. Those plug-ins allow you to watch video, listen to music, play games, read documents, participate in web chats, and even download data faster—all from inside your web browser.

Plug-in A piece of software that adds functionality to another program.

Your current computer probably came with a number of plug-ins, like Adobe Flash Player, pre-installed. Flash may actually be the most used web browser plug-in in the world. Many websites, like YouTube and Hulu, won't work without Flash. Neither will many Facebook applications and most online games. Some plug-ins like Flash, QuickTime, and Real Player, accommodate multi-media applications. Others provide functionality in security, encryption, and a wide range of other areas.

The great thing about web browser plug-ins is that anyone can write and distribute them. Big companies like Adobe, Google, and Microsoft develop plug-ins. So do small companies and some individuals. In general, web browser plug-ins make the Internet better.

What's the down side? Like your Internet browser itself and your operating system, the plug-ins that you use are updated from time to time. Sometimes these updates add new functions. Sometimes the updates remove security holes that were overlooked in the previous version. In either case, from time to time you're going to be notified that you need to update a specific plug-in in order to use your favorite site. You're probably used to this.

Most of the time, when a website requires a newer version of a plug-in to work correctly, it also provides you with a convenient link to download that update. Most of those links are just what they appear to be. Unfortunately, a small number aren't. Some sites are now using fake notices about updating plug-ins as a way to trick users into downloading malware. If you use the provided download link, you may not get the latest version of Real Player. Instead, you may get spyware or a Trojan that allows your computer to be drafted into a bot army.

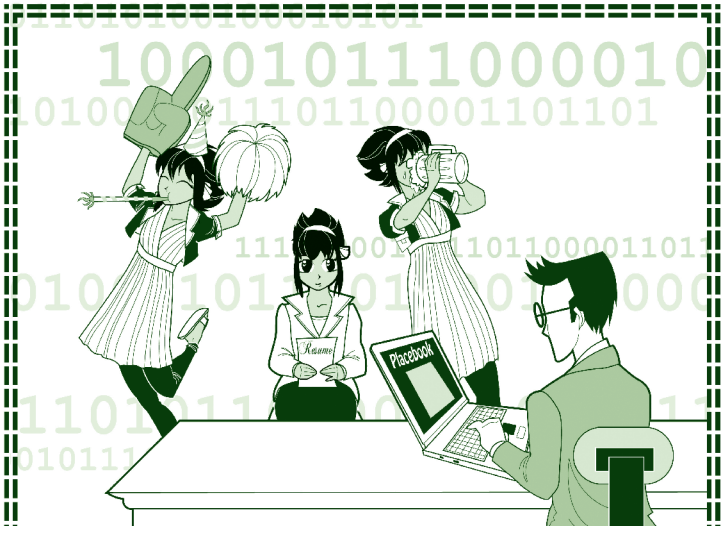
So, how do you avoid the risk and still get the benefits of plug-ins? First, determine that the plug-in itself is legitimate. If a website you don't know well is demanding that you download a plug-in you've never heard of, be wary. If the plug-in is legitimate, always get your updates from the source. While it might be convenient to hit the embedded link for the latest Flash update, it's always safer to go directly to Adobe's website.

Chapter 10

Private Blogs and Public Places

I spent this morning reading my oldest daughter's online diary. And that of her younger sister. Her cousins. Her best friends. Her boyfriend...

How'd I get there? I did a 5-second Yahoo! search on my daughter's boyfriend's name. The first site that came up was his Xanga blog. It didn't take long clicking through his Subscriptions to find my daughter's blog. From her blog, I meandered through the online musings of her friends. And their friends. Each new blog gave me links to the next. I'm starting to feel like I've spent the morning reading the diaries of half the kids in this county.



I won't tell them, of course. None of them gave me their links and I'm ABSOLUTELY sure they weren't meaning for me to read the stuff they posted. The content was really eye-opening. I'm still floored by some of the incredibly personal things the kids said. It's like they think they're the only people living on the Net. I have to wonder how they'll feel about those same comments when they've grown out of adolescence but their teen musings live on in perpetuity in cyber space...

—Anonymous Mom

Unless you're a pretty atypical teen, chances are that you know about blogs, at least in the abstract. Fourteen percent of American teens actually keep a blog. An even larger number "blog" their experiences on integrated social networking sites that include blogging features. What's the difference? A blog is much more detailed, and definitely more text based. Social networking sites limit "status" entries (which mimic blog entries) to roughly a short paragraph. That's more than a tweet, but definitely less than a blog. A traditional blog entry looks more like a 5-paragaph essay. That probably explains why only 14% of teens keep regular blogs. As Tom Ewing points out in *Teens Don't Blog?*, "Voluntary writing at length is always going to be a niche, no matter how easy it is to do, and it's not surprising that the much faster moving and more social world of status updates is more attractive to more people." Still 14% is about one in six and those 60 million status updates posted to Facebook each day have the same limitations and dangers as their longer cousins.

If you're one of the teens who keeps a blog (or regularly posts status updates), have you thought about what types of things it's OK to post? Or wondered what will happen to your postings in years to come? In this chapter, we talk about the implications of having an online blog and how to do so without compromising your safety or your future. We'll also talk about the history of the blogging community.

10.1 So What's a Blog?

A **blog** is short for "weblog"—a website that consists of a series of data entries. Much like an online journal or diary, some blogs are standalone. That is, they don't link to other sites. However, most blogs contain links to other blogs and sites of interest. While it can look, and sometimes function, like a diary, a blog is really a very public record. In fact, one of the problems with blogs in terms of protecting individual privacy is that too many users seem to treat them as if they really were private diaries instead of public records.

Blog A web-based log containing text entries ordered by date (like a journal) as well as links to other sites.

In industry terms, blogs are a fairly recent phenomena, dating only from the mid- to late-1990s. According to some experts, the first blog appeared in 1993, but

there's some question whether *Mosaic's What's New Page* really meets the criteria of a blog as we understand it today. While it certainly did contain the expected links to other sites of interest, it also lacked the personal "diary-style" touch that defines the essence of today's blogs.

Some experts date the first blog to 1997. That was when John Barger actually coined the term weblog to describe his *Robot Wisdom Weblog*. Another blogger, Peter Merholz, later shortened "weblog" to create the term "blog" that we use today. As you'll note from the incredibly hard-to-read screenshot, this was long before the free web-log creation programs that simplify creating crisp web pages that are easy to read and navigate.

John Barger's Robot Wisdom Weblog
http://www.robotwisdom.com/

Today, blogs are much more polished and considerably easier to create. With the advent of free blog creation programs, bloggers no longer need to understand **HTML**—the programming language used to create web pages—or really have any knowledge of even basic web page creation.

HTML HyperText Markup Language. The programming language used to create web pages.

10.2 Blogging Makes the Big Time

While blogging dates to the mid-1990s, it didn't really take off until Prya released the tool Blogger, which allowed less savvy users to create and maintain blogs without becoming webmasters in the process. Blogger expanded the blogging community from a few dozen techno-elites and opened the door for the rest of the Internet community.

Top Teen Blogs

If you're looking to create your own blog, or just want to read blogs probably written by other teens, here's a few good recommendations on where to go:

- Xanga
- LiveJournal
- Blogger.com

Even teens who take an alternate path can find an online blogging community at HomeschoolBlogger.com.

The rush of would-be-bloggers through that door was astounding. In 1999, Jesse James Garrett, editor of *Infosif*, published a website listing all of the blogs known to exist at that time. There were 23. Today, there are millions. According to Technorati, a tracking firm in San Francisco, a new blog or two is created just about every second of every day.

Bloggers discuss everything from yesterday's social studies test to international events and national policy. Political blogs have taken off to the point that some bloggers were issued official press passes to cover the major party conventions preceding the last two Presidential Elections.

For most teens, however, maintaining a blog rates much closer to keeping a public journal than being part of the media establishment. As such, teens tend to keep their blogs within mostly teen friendly environments.

10.3 Say WHAT?!!!

Blogging has become an apparently permanent part of the teen culture. That's not necessarily a bad thing. Teens have some pretty intense philosophical discussions in some of those blogs. Kevin Krim, head of subscriptions at the company that owns blog-site *LiveJournal*, points out, "For every off-color picture you might find, you are also going to find a number of kids having really interesting

conversations about their developing views of spirituality, what they think about war. Those are good things to be thinking about."

The trick with blogs, as with all areas of Internet technology, is to keep the good while avoiding the clearly bad or dangerous. The good part is that blogs provide an easy, motivating forum in which teens hone their wit, unknowingly practice their writing skills, and essentially document their adolescence. However, as Elizabeth Armstrong pointed out in the *Christian Science Monitor*, while a blog may be an easy online diary, it's a diary to which "the rest of the world now has peeping rights."

With blogging, a truly dangerous area is that kids provide FAR too much personal information. A substantial number of teen bloggers include their full names on their sites. Over half publish their locations or contact information. If the only people reading their blogs were other teens, that might be OK. Of course, they aren't. Putting personally identifying information in your blog can put you at considerable risk from unsavory characters online.

Of course, there's always the danger of creepy characters anyplace a large number of teens gather. And blogs are certainly one of those places. Mary Ellen Handy, a middle school technology coordinator, reports that a full third of her 250 students keep blogs. That's expected. What's frightening is that only 5% of those students' parents knew that. While that low number might surprise you, it undoubtedly wouldn't surprise Edward Parmelee, a special agent with the FBI's Jackson Mississippi cyber crime squad. A frequent speaker at schools, Parmelee notes that when he mentions blogging to parent groups, "We get these deer-in-headlights stares. They don't even know what we're talking about."

Blogging No-No's

Be a safety-conscious blogger! Never post:

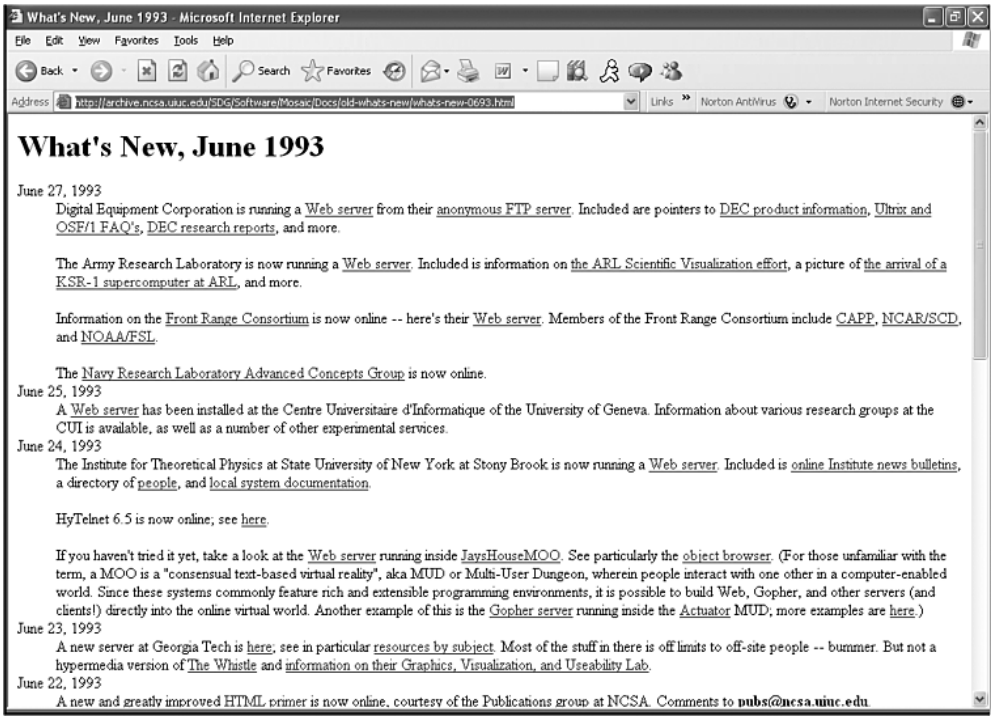
- Your full name
- Your address
- Your phone number
- Your age
- Anything you wouldn't want your mother to see!
- Anything you wouldn't want a future employer to see
- Anything that could compromise your college acceptance

If your parents are among the uninformed, this could be your chance to bring them up to speed. While you may not want them reading your own blog on a regular basis, your parents are your first and best defense. You should keep them in the loop enough to allow them to help you make good decisions for your own protection.

10.4 Object Permanence

Another problem with the proliferation of teen blogs is that most teens have no idea just how long those blogs will be around. That could be a very, very long time.

If you're wondering just how long those old blog entries you've made can hang around, have a look at the screen shot below. These are the entries made on *Mosaic's What's New Page* at its inception back in 1993.



Mosaic's What's New Page, June 1993
http://archive.ncsa.uiuc.edu/SDG/Software/Mosaic/Docs/old-whats-new/whats-new-0693.html

Unlike physical diaries or journals, blog entries are public creatures, not private. Once you've added a new entry to your blog, those words become easily accessible to nearly every person on earth who has Internet access. Many blogs are completely open, not even requiring readers to log in. Xanga.com, a popular teen blogging site, is exactly like that. The anonymous mom in our case study at the front of the chapter didn't need to actually log into Xanga to read her teen's online postings. She simply ran a quick Yahoo! search.

Even sticking to sites that limit access to other members hardly restricts access to your blog entries. Just how difficult was it for you to create a free blog online? What makes you think that your mom, your school principal, or even a prospective employer 10 years from now couldn't do the same?

10.5 Bloggers Eat Their Own

While teens maintain blogs that are often a bit too personal, they are still, for the most part, fairly positive. Some of the supposed grown-ups in the **blogosphere** aren't quite so well behaved. An unfortunate side effect of the growth of the blogging culture has been the emergence of the attack blog.

Blogosphere The blogging community as a whole. This includes all blogging forums, blogging sites, and individually maintained blogs.

Attack blogs exist partly, and sometimes wholly, to say unpleasant things about others. Sometimes they attack political adversaries. Other times, they take aim at competitors. Or simply people or products the blog writer just doesn't like.

10.5.1 Attack Blogs

Negative blogs, often called **Attack blogs**, surfaced as a major problem as far back as the 1990s. Often taking the form of "attack-the-company" websites, attack blogs began as a way for dissatisfied customers, unscrupulous competitors, and disgruntled former employees to attack firms using a wide platform and relative anonymity. Thanks to a spate of lawsuits, that particular tide of accusations has abated. In its place, the darker side of the blogosphere is now sporting a host of personal attack blogs.

Attack blog A blog written specifically to attack an individual, company, or group.

Personal attack blogs are simply another media for cyberbullying and generally take one of two forms. The most obvious attack blogs are blatant attacks on a specific person. This could be negative statements on another teen's blog, or even an entire blog devoted to trashing the victim. One such blog, called *Kill Kylie, Incorporated*, was filled with vulgar accusations against then 8th grade Kylie. (Kylie was so distressed by the attack blog, apparently put up by schoolmates, that she eventually changed schools.) The less obvious attack blogs are designed to look like they're written by the victim. The idea is to trash the victim's reputation by making it look as if the person is admitting to something horrible like killing cats in their spare time or lobbying in favor of child pornography.

If you are the victim of an attack blog, chances are that you know your attacker. A National Children's Home study found that almost three-fourths (73%) of cyberbullying victims know their attackers. While your first instinct may be to respond to the attack with your own posts, or even your own opposing blog, that's often not a good idea. If you want to hush up a nasty rumor, it's probably not in your best interests to scream back at someone sitting on a very large and very public soap box. And, that's a pretty good description of where attack bloggers sit.

This is something to think about if you find yourself considering, or in the midst of, a blog battle. Take the advice of Robert Mahaffey, a cyber crime investigator for the Mississippi Attorney General's office. "The Internet is the wild, wild West of the 21st century, and it should be viewed that way." Thankfully, attack bloggers are a very small minority of the blogging community. Daniel Lyons points that out on Forbes.com, noting that "Attack blogs are but a sliver of the rapidly expanding blogosphere." Of course, gun slingers and outlaws were also a small part of the old West. That didn't mean that they weren't a real threat. Attack bloggers are a similarly dangerous minority. Taunting them by posting back definitely isn't very wise.

While responding online often just encourages the attackers, that doesn't mean you should simply ignore the attacks. Your best bet is to report the abuse instead. Blogging sites now ban attack blogs so you may be successful in having the offending site removed. If your attackers are still in school, you may also find recourse

through official school channels. Many schools have bans on attack blogs—even when written outside of school hours. For more information about how to better protect yourself, read *Chapter 6, Cyberbullying*.

10.5.2 Legal Repercussions

Another good reason not to respond to attack blogs is that you don't want to be dragged into any ensuing legal battles. When adults begin throwing unsupported accusations at each other, the inclination on all sides is to run for a lawyer.

Libel (publishing statements that you know to be untrue) is not only ungracious, it's illegal. If you're convicted of libel you could find yourself forced to pay for any damage that you caused to your victim's reputation or livelihood. This can be very, very expensive. Let's imagine that you decide to really trash a company's new weight loss product. You announce in your blog that not only did you not lose any weight, but you blew up like a balloon and developed a nasty rash across your face. You even post a photo of poor you with the horrible rash that was all their fault. Now, let's imagine that you actually got that swelling and rash by being stung by a wasp. You just used the picture to get back at them because you read somewhere that they were using animal testing on their products. Your motives might have been honorable, but your postings still constituted libel. If the company sued you (and they just might if you damaged their sales enough), you could be on the hook for all the money they could have made in the next twenty years if the reputation of their product hadn't been trashed.

Are you likely to be convicted for nasty comments that you make in your blog? Probably not. On the other hand, you're not likely to go to jail for stealing your neighbor's newspaper every morning. Keeping your web postings honest (and your hands off of your neighbor's news) is just the right thing to do.

10.6 Thinking Ahead

Like email (which often stays on your ISP's mail servers long after you've deleted your copy and forgotten its content), blog entries also don't really go away when you've moved on and forgotten about them. They live on in backup drives and archive files. They may even live on sitting on someone else's website. How often

have you copied something you found especially profound or funny and pasted it into your website? Someone else out there may have done the same thing with your postings.

Throughout history, teens have always done and said stupid things they've come to regret as they entered adulthood. What's changed is that Xanga blogs, YouTube movie clips, and MySpace photos can now document those mistakes—maybe forever.

In recent history, a number of persons nominated to the U.S. Supreme Court have been forced to withdraw over allegations of poor decisions that they made in the 1960s. Just imagine if those decisions had been documented online by the nominees themselves. In 30 years we could have Congressional Committees skip the FBI checks on prospective jurors and turn instead to the archive files of old blogs. Given some of the teen blogs we recently read, we can envision a Supreme Court filled with nine empty chairs. At the very least, there'd be an awful lot of thoroughly embarrassed grandparents. Don't be one of them.

10.7 The Right Way to Blog

We hope this section doesn't sound too negative. We're really trying to avoid the "big hairy monsters on the Internet" tone. Because our job in this book is to give you the information you need to help protect you from the nasty side of cyberspace, that's a little bit unavoidable.

Still, we don't want to leave you with the idea that blogging is a bad thing. It's not. We realize that your blogs are an important part of your online existence. Your entries over time can show a clear record of your emotional growth, a web-based documentary of your development into a thoughtful, exciting individual.

To take advantage of the boons of the blogosphere, you just need to follow a few simple rules:

- **Be honest.** This means you should maintain your integrity on several levels. Obviously, you should only publish blog entries you know to be true. You should also be honest about yourself. If you need to lie about your age to participate in a particular blogging forum, you know in your heart that you

really shouldn't be there. There are blogs that are open to teens of all ages. For your own protection, stay out of the forums intended only for adults and teens older than you.

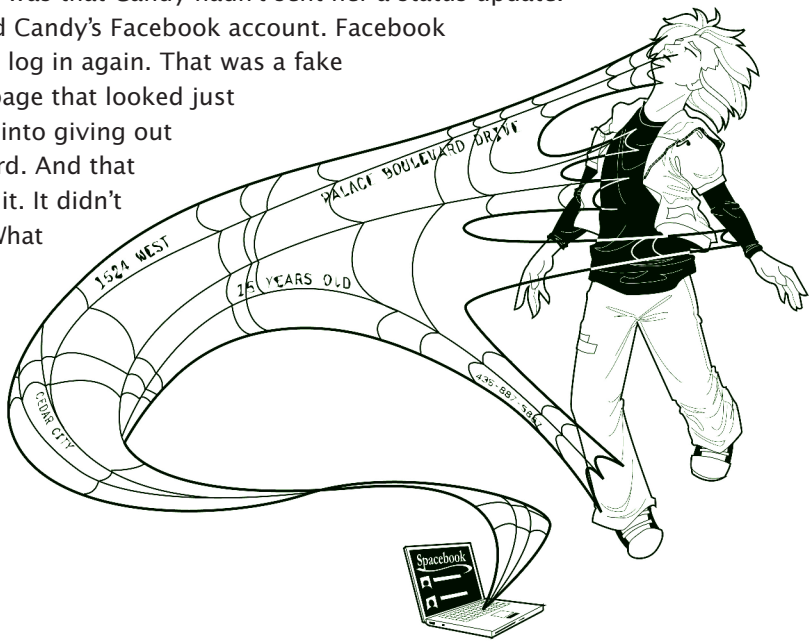
- **Don't be too honest.** There are some things your blog audience really doesn't need to know. These include any bits of information that would personally identify you. Your name. Your address or even the name of your town. Your school name. The full names of any friends or acquaintances. For your own protection, you need to keep your personal information off the Net.
- **Use discretion.** Always remember that your blog is a PUBLIC record. Don't post anything you wouldn't be comfortable sharing with Grandma over dinner at Thanksgiving.
- **Think ahead.** Never forget that your blog entries may very well outlive you. Before you post something, ask yourself how you'll feel about that entry next month or next year. Or well into the next decade. Do you really need to blog this, or can you skip it and go talk to a friend in person?
- **If you can't say anything nice…**

Chapter 11

Going Social

High school senior Miranda has always been a photo hound. Her mom kids that she's been hamming it up for family shots since before she could walk upright. So when Miranda got a status update on Facebook from her friend Candy announcing, "My friend caught you on hidden cam..." she just *had* to look. Funny, her computer wasn't behaving at the time. She had to log in to Facebook again, even though she'd just logged in a few minutes before. Then she couldn't view the photos until she downloaded a new version of Flash...

What Miranda didn't realize was that Candy hadn't sent her a status update. A nasty worm had accessed Candy's Facebook account. Facebook also didn't want Miranda to log in again. That was a fake screen, displaying a login page that looked just like Facebook's to trick her into giving out her user name and password. And that Flash update? You guessed it. It didn't link to Adobe Flash at all. What Miranda downloaded was rogue security software. Minutes later, she was seeing pop-up windows informing her that her computer was infected with spyware and it would only cost her $49.95 to upgrade her security software to get rid of it...



Like many users before and after her, Miranda was scammed by malware targeting social networking sites. In this case, the worm distributed a link to a fake login screen to phish her password, then tricked her into downloading a Trojan which kept directing her browser to fraudulent websites that pushed rogue security software. In less than 15 minutes, Miranda managed to get hit with almost every variation on malware!

Right now, scammers are targeting social networking sites big time because that's where people are spending more and more of their time online. Why so popular? Social networking is what the pundits call being part of an online community that facilitates connections between users. Obviously, there have been places to meet and discuss issues with online "friends" since the Internet began. However, the early bulletin boards and discussion groups were limited. Users posted their opinions and often responded to the postings of others, but they didn't grow their communities in the same way as today's social networks.

11.1 Where the Friends Are

In 2003, MySpace became the first major **social networking site**. Based on an earlier, less developed site called Friendster, MySpace hit the big time in a big way. By 2010, the U.S. site sported over 70 million users. Factoring in MySpace sites for 30 countries worldwide, plus specialty sites like MySpace Latino, that's about 125 million MySpace users.

Social networking site A website that allows users to define relationships between themselves and network among not just their own friends, but friends of friends, and friends of friends' friends—ever expanding their online network.

Hardly the first social networking site, MySpace was the first to "go viral" in terms of coming to the attention of the general public. While users are technically "required" to be at least 13, the requirement is based on self-reporting of age.

MySpace users, while dedicated, often also have accounts at other social networking sites, like Facebook. Facebook was started in 2003 by Harvard sophomore Mark Zuckerberg as an online version of the college facebooks. These were photo books issued for each freshman class (at smaller schools) or each dorm (at larger

universities) to help new students get to know each other. At the time, Harvard didn't have a student directory with photos and web mythology credits the site with 22,000 photo views in its first four hours online. The response was so high that Zuckerberg launched an official site, limited to Harvard students, in 2004. Within a month, half the undergraduate student body had registered.

It wasn't until September 2006 that Facebook opened membership to anyone 13 or older with a valid email address. By mid-2008, Facebook was running neck to neck with MySpace, pulling ahead worldwide in November 2008 when Facebook drew 200 million unique worldwide visitors. That month, over 20% of Internet users visited Facebook. By August 2010, Facebook alone reported 500 million active users.

While MySpace and Facebook most certainly dominate the market, they are far from the only social networking sites frequented by teens. Other popular sites include Friendster, Yoursphere, and Bebo. Altogether, those sites boast enough users to populate a Latin American country. By 2009, 72% of teens and young adults used at least one social networking site.

11.2 Friends: Real and Virtual

"Friending" and being "Friended" are incredibly important concepts to understanding the social network scene. When you register for an account at MySpace or Facebook, the service offers to look up all the email addresses in your web-based email and compare those addresses against actual Facebook users. In 2010, the average Facebook user had 130 Friends.

Poke Hitting Poke in Facebook lets another user know you'd like to get her attention. She can poke you back, write on your wall, or even ask to Friend you.

Collecting "Friends" is both the greatest advantage and the weakest link of online social networks. Because of privacy controls, most of the Profile information you post on social networks is viewable only by other users that you've designated as Friends. The danger comes when teens eager to appear popular accept Friends that they don't really know and post too much information thinking that only their

friends will see their page. Sixteen-year-old Eric from Novato, California thought it was really cool to have 1,700 friends. In reality, some of those friends could just be creeps peeking around at your life. Further, malware has been created to exploit that trust on social networks. Naïve users who believe that only their friends have access to their postings are often appalled when those postings are captured, re-posted, and circulated to people they never would have wanted to share them with.

11.3 Groups

Both MySpace and Facebook have official policies against "Harmful content" as well as content deemed offensive or abusive. While these are great policies in theory, the practice leaves much to be desired, especially in the area of Group content.

Facebook alone sports thousands of groups which allow members with similar interests to meet and network—purportedly the actual point of having a social networking site. These groups include scores of innocuous Fan Clubs like "Addicted To Project Runway" and rather imaginative whimsical groups like "Physics doesn't exist, it's all gnomes." Some even sound a bit desperate, like "We need to find a kidney donor for our father. Help us spread the word." Or promote a political or heartfelt religious sentiment.

Unfortunately, other groups seem to live on the dark side. In the first 10 minutes of scanning groups to prepare this chapter, we had occasion to report no less than 12 groups to Facebook for violations including nudity in photos, obscenity, and vulgar language.

In addition to general smut, a bigger problem rests in the intended content of many of the groups. Even if you discount the heavily questionable content of some of the groups categorized under Sexuality, you're left with a large number of groups that glorify underage drinking.

Friend to All

Feeling friendless? Whatever you do, don't compare yourself to Tom Anderson.

Co-founder of MySpace, 34-year old Tom is the "default" friend given to all new MySpace users. By April 2010, Tom had over 12 million friends.

In their defense, keeping social networks clear of bad content given their millions of users must be a daunting task indeed. Even if such entries are removed within hours, the constant postings of new users would still provide a nearly endless stream of objectionable material.

11.4 Third-Party Apps

A social networking application is a separate program that works within the social networking site to provide additional functionality. Because these functions are written by independent companies, they're referred to as third-party apps. If you've used Farmville, played Scrabble, or sent a birthday card on Facebook, you've used a third-party application. If you haven't used one, you're in the minority. Facebook reports that 70% of active users access third-party applications each month. Hardly surprising given that there are over 500,000 applications!

Because third-party applications are run by companies other than your social networking site, using them has implications for your privacy. When you agree to use a third-party application, you're giving that party permission to access at least some of your Facebook or MySpace information. According to the Facebook Terms of Service, "When you add an application and use Platform, your content and information is shared with the application. We require applications to respect your privacy settings, but your agreement with that application will control how the application can use the content and information you share." This means that you need to carefully read the user agreement when you add a new application. Not concerned? You may not realize just how much information you're giving away. In addition to a list of your Friends, your user information could include your name, profile photo, birthday, political views, hobbies, interests, relationship status, education history, and work history as well as copies of all the photos in your Facebook site photo albums. In the hands of an unscrupulous advertiser, that's a gold mine.

Sometimes, an application provides MORE than you asked for. In early 2008, it was learned that a popular Facebook application known as *Secret Crush* was delivering adware from Zango. While Facebook put a stop to that, in many respects they're playing the same game that you are with malware—they're just playing on

a much larger scale. Facebook changes their policies and attempts to block obvious malware, phishing attempts, and adware. The bad guys look for loopholes in the legal writings or software to get around the new rules. As the victim in the middle, it's your job to beware of scams and keep track of what you're agreeing to and with whom.

11.5 Phishers of Friends

By 2009, phishing expeditions on social networking sites became a nearly daily event. Some of the more memorable were FBAction.net, Koobface, and Areps.at. Most of these phishing scams took the form of status postings containing embedded links. If you clicked the link, you were routed to an outside website where you saw a Facebook login screen that looked almost exactly like the real screen. If you bit and logged in a second time without thinking about it, your Friends would soon receive a status posting with an embedded link. To add insult to injury, the outside website often infected your computer with adware.

These types of phishing attacks are especially on the rise. Knowing what we all know at this point about phishing attacks, why do so many people still fall victim? The attackers rely heavily on social engineering. While users have learned to be very cautious about links embedded in emails, we tend to be very trusting of links embedded in postings from Friends. Basically, the phishers exploit our natural tendency to trust our own friends. For even higher click through, attackers use postings guaranteed to pique your interest. The Koobface attack on MySpace and Facebook in 2009 generated status updates like *Paris Hilton tosses dwarf on the street* and *My friend caught you on hidden cam. Have a look!*

11.6 Posting Too Much Information

Most teenagers post a lot of very personal information online. This can have long-lasting consequences that you may not have thought about. According to Career-Builder, about 30% of employers search social networking sites to check out new hires. And a third of hiring managers report turning down an application because of information they found online.

Experts disagree on whether employer screening of social networking sites is good or bad. On the plus side, ambitious teens can use social networking sites to present their better sides by including photos and postings about extra-curricular activities and volunteer work. On the down side, students often post a lot of personal information that employers aren't allowed to ask about because they can't legally use that information to make a hiring decision. Those details can include a job candidates' gender, age, race, religion, political views, physical or mental disabilities, and sexual orientation. It isn't just racy photos you need to worry about. That photo of you at a Gay Rights March or a Pro-Life Rally could seriously offend a potential employer. Should they make hiring decisions based on that type of personal information? Not really. The problem is that once your information is public, it's public.

To protect your personal information, take Facebook's own advice and "Control every time you share." On all of the social networking sites, you have the option to lock-down your profile and limit access to your personal information and photos to just your Friends. In many cases, you can even select a subset of Friends.

11.6.1 Questionable Photos

People who love social networking sites LOVE photos. Facebook reports that three *billion* photos are uploaded to its site every month. That's a lot of birthday parties, anniversaries, and graduations. That's also billions of opportunities for users to post photos that they probably should have kept to themselves (or never taken in the first place!).

Online photos are a great source of entertainment—especially for personnel directors and job recruiters. As Allan Hoffman, a Tech Jobs Expert at mega-employment firm MONSTER points out, "It's not just what you say that can be held against you when you're looking for a job. It's also what you post on MySpace, write in your blog and broadcast on YouTube." Photos from last year's homecoming dance that entertain your friends today could keep you from being hired in the future.

Photos can also allow stalkers and pedophiles to identify you. To protect yourself from all of these dangers, be very careful about what you post online. Also try to

keep tabs on the photos others post of you in which you're identified ("tagged"). By tagging photos, your friends can easily identify you to the world within photos you'd rather not share. ***Real*** friends aren't determined to make you look foolish online.

11.6.2 Dangerous Webcams

Webcams present all the dangers of digital cameras and then some. A frightening recent phenomenon has been the advent of pedophiles on social networking sites offering teens money to take off their clothes and perform inappropriately in front of their webcams. Justin Berry was just 13 when he was propositioned by a pedophile. For the next five years, he used his webcam to basically work as a child prostitute.

While it is unlikely that your webcam will turn you into a prostitute, it is likely at some point to make you look like an idiot. Silly pranks make home movies endlessly entertaining when shared with family and close friends—people who know you and love you and find it funny because the behavior on film is so *unlike* you. Strangers don't see videos that same way. They're laughing AT you, not with you. Again, use discretion with anything you put online. Consider how you'll feel about that video when you're 30.

In the meantime, having a webcam in your home may seriously compromise your privacy. Imagine how surprised Blake Robbins was to discover that his high school had activated a webcam in the school-provided laptop and was spying on what he did in his own bedroom. Blake became aware of the spying when the school disciplined him for suspected inappropriate behavior and provided as proof a photo the laptop webcam had taken of him without his knowledge. Fellow students were stunned. Savannah Williams, a sophomore at the same school outside of Philadelphia was very distraught, pointing out that she often took her laptop into the bathroom with her to listen to music while showering.

11.6.3 YouTube

Webcams allow you to embarrass yourself in front of all your social networking Friends. YouTube lets you share that humiliation with perfect strangers.

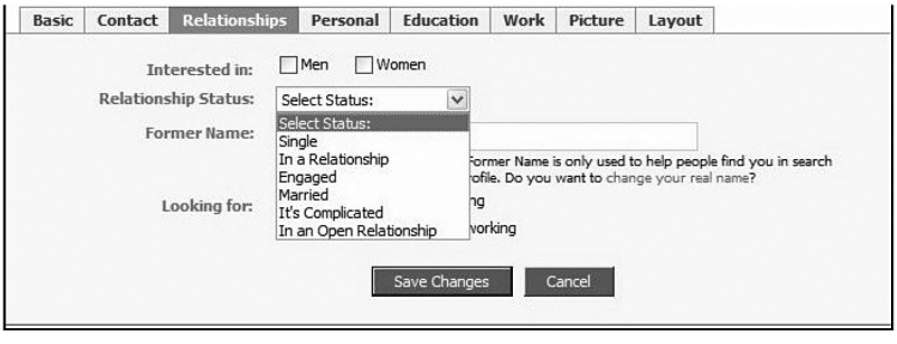
We've all seen YouTube videos that were hysterically funny. To us. But when they're viewed millions of times, those funny videos can really damage their

subjects' self-esteem and mental health. Imagine how you'd feel knowing that millions of perfect strangers were laughing at you. That's only funny when it happens to someone *else*.

Mental health isn't the only issue either. The would-be producers can easily get carried away. One mom reported in 2009 that her 15-year-old son and his friends had produced some seriously disturbing videos for YouTube. "They had everything from silly stunts to self-injury like stapling themselves and pouring rubbing alcohol on their hands and lighting it with a lighter." Was her son a problem kid? Not really. He was trying to be creative and felt that he needed to be extreme in his video to get attention online. He's lucky he wasn't permanently injured.

11.7 Breaking Up Online

Another thing to keep in mind about social networking sites is that more and more they take the place of people actually meeting, talking, and connecting on emotional issues. In researching this book, we've heard from a remarkable number of teens who tell us they've been dumped at least once on Facebook. How does this work? Facebook provides a relationship indicator. When you enter your profile information, it allows you to define your **Relationship Status**.



Today, those emotionally underdeveloped partners who would have slunk off without calling in years past simply change their **Relationship Status** online. Far too many a committed partner now learns from a friend that their significant other is now listed as **Single**. This brings up probably the best indicator of whether you're

really ready for online social networks—self-confidence and maturity. Are you self-confident enough to handle being dumped online? Even better, are you mature enough NOT to do that to someone else? We saw one teen devastated when his best friend told him that Suzie (his girlfriend for four years) had changed her relationship status to **Single**. That's not cool. It's cruel.

11.8 Tweet, Sweet

Created in 2006, Twitter is a social networking site that specializes in microblogging. That's heavy on the "micro." Twitter updates, called tweets, are required to be short and sweet.

```
Tweeting is the social networking equivalent of text messaging. Each "tweet" can
contain no more than 140 characters... This "tweet" is exactly 140 characters long...
```

Often jokingly referred to as blogging for the sound-bite generation, Twitter was designed for users on the go who were posting from cell phones and other mobile devices. That's actually the reason for the short status limit. Cell phone text messages are limited to 160 characters, so Twitter limits tweets to 140 characters, leaving 20 characters for author attribution.

Like other social networking sites, Twitter works with third-party applications. 50,000 of them by 2010. It's also susceptible to many of the malware and phishing attacks directed at the other social networking sites.

Twitter has also been a target itself. In 2009, 184+ million users were locked out on several occasions due to denial of service attacks aimed at the site. Some pundits speculated that Twitter was targeted because the site has been aggressively filtering URLs to block those used in malicious tweets, reducing the malware writers' income. Sometimes, even when you win, you lose.

11.9 Tips for Staying Safe and Social

Scammers are targeting social networking sites because that's where people are spending their time online. Here are some tips for staying safe:

- Watch out what you post. Don't reveal your full name, address, phone number, or school.

- Stay in your age group. If you're 13, don't pretend to be 19. That could put you in conversations and discussions that are uncomfortable because you're not quite emotionally ready for them.
- Don't post content you wouldn't want your parents to see. Remember that information you post today could come back to haunt you when you are trying to get a scholarship or a job.
- Understand the privacy settings for the social networking site you use. Then use those privacy settings!
- Even if you lock down your profile and define your postings as private, don't assume that no one can see them. Some malware specifically targets "private" pages.
- Remember that you're not the only person you know with a camera or webcam. Keep tabs on any photos or videos your friends are posting that might feature you.
- Don't take Friends at face value unless you've actually looked at their faces. That 16-year-old girl you met online might be a 65-year-old man.
- Don't let anyone talk you into doing anything you find creepy or feel uncomfortable about. That especially means anything that involves your webcam. Inappropriate videos NEVER go away. Just ask Paris Hilton….
- Never ever meet anyone F2F for the first time by yourself. This is pretty self-explanatory but the most critical deterrent to online creeps. Don't put yourself in a dangerous situation when you don't need to.

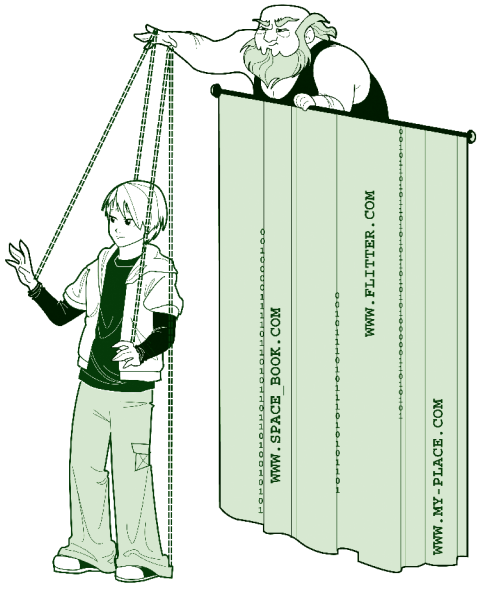
Chapter 12

Friends, Creeps and Pirates

A typical teenager from Michigan, Mindy spent a lot of time on the Internet—much of that time with online friends. Over a period of five months, she spent a lot of time in particular chatting with "George", an online friend from London.

As she got to know him (or so she thought), Mindy learned that George was having some problems with money. Banking issues, family arguments—really complicated stuff related to British banking laws. He had tons of money, of course; he was just having a hard time getting access to it. Mindy could fix this for him. All she needed to do was to cash a few money orders and send the cash back to George. Naturally, she should keep a few hundred dollars for her troubles.

A money order is like a bank check used by people who don't have a bank checking account. You can buy a money order using cash at any post office and most convenience stores. Many people use money orders; some Internet sellers actually require money orders for payment because it's safer to accept a money order from a stranger than it is to take a bank check. That's because a money order is paid for in cash. It can't "bounce" like a check can if the person's bank account doesn't contain enough money to cover the check.



Knowing that money orders are safe, and wanting to help her friend, Mindy agreed to cash the money orders. Luckily for her, the Post Office realized right away that the money orders were fake. Even luckier for her, they opted to go after George instead of pressing charges against her.

"George" of course, knew full well that the money orders he tricked Mindy into trying to cash were all counterfeit. Not that it's likely that George was his real name. Or that he actually lived in London. Or that any of the myriad details on his life that he provided to Mindy those five months were actually true. In real life, George could very well be a 60-year-old woman running a counterfeiting ring from Eastern Europe. About the only "fact" that Mindy knows for sure at this point is that George was most definitely a creep.

Unfortunately, the Internet has many scammers. According to postal inspector Fred Van De Putte, the money order scam is especially common. Other online criminals are identity thieves. Their goal is to get to know you well enough to take over your identity when you're not looking. Other creeps are even worse—pedophiles pretending to be teens to find new victims.

To avoid becoming a victim, you need to be aware of just what you can and can't tell about online acquaintances. And, what you should and shouldn't tell to those same people.

12.1 Meeting People Online

The Internet is a wonderful tool for keeping in touch with old friends and meeting new people who share your interests and goals. Where else could you find a ready-made community of people who love the same music, *American Idol* fans, or even a comforting support group for overweight teens or young girls struggling with body image issues? For troubled teens, the Internet provides many opportunities for seemingly anonymous help with serious problems they're too afraid or embarrassed to discuss at home.

The problem is that people who want to "help" aren't always what or who they claim to be. The fellow "teen" you can really talk to about your life may not even be a teen. Just ask Amy, a 14-year-old from Seattle. Amy was having family

problems and was thrilled to find another teen online who understood exactly what she was going through. After months of baring her soul online, 14-year-old Carl offered to help her run away. Throwing caution (and common sense) to the wind, Amy joined Carl on a bus heading to Missouri. The longer they traveled though, the less sure Amy was about Carl. During a short stop on their route, Amy had the chance to rummage through Carl's wallet. What she learned was that 14-year-old Carl was really 27-year-old Robert. Miraculously, she was able to escape his company and was returned to her parents. As for "Carl," he's probably still out there and still pretending. Much to the disgust of Amy and her parents, he was never charged.

Amy learned a very hard lesson in an extremely dangerous way. Today, she still uses the Internet but only under close supervision by her parents. For those times they're not in, her father has installed monitoring software and makes it a point to know who she's talking to and about what.

Is Amy's story unusual? Yes and no. Taking the risk of meeting online friends **F2F** (Face to Face), is something that few Internet users attempt. The specter of teens baring their souls to perfect strangers is unfortunately far too common. Are you likely to have Amy's awful experience? Probably not. Truthfully, most of the people you meet online really are who and what they claim to be. But the reality is that just as creeps exist in real life, those same creeps exist online. Are they hiding behind every other screen name? Hardly. But there are enough of them that you need to understand just how easy it is for them to lie and hide behind a digital face because you can't see them.

F2F A Face to Face meeting (in person) with someone you've met online.

12.1.1 Where Creeps Hang Online

There's a common fallacy that creeps spend their time online in racy chat rooms and sleazy online communities. That may be true, but those are certainly not the only places they hang out. Savvy con artists and pedophiles look for easy marks. The more naïve their quarry, the better their odds.

Keep this in mind as you chat online and don't assume that all visitors to "wholesome" forums are themselves wholesome. Fourteen-year-old Amy made exactly

that mistake. Explaining why she took Carl at his online face value, she explains, "I assumed because it was a Christian chat room that there would be mostly Christians in there. So, basically it would be like a regular conversation with people." Pedophiles generally don't have CREEP tattooed on their online profiles. They also make it a point to be where they're most likely to find vulnerable teens. Don't be surprised to find them in church-related chat rooms, online religious communities, scouting themed groups, social networks, and other "wholesome" teen forums.

12.1.2 Protecting Yourself from Creeps

It is easy to meet new people online. Your friends will introduce you to their friends, and their friends, and so on. Before you know it, your digital network is HUGE. It might seem easy to talk to people online because you feel safe. No one is in front of you judging how you look, talk, walk, or part your hair. You can never take meeting someone over the Internet lightly, however. If you don't know that person in real life, you have no idea who he or she really is. You may even feel "connected" to your new friends, but you need to keep in mind that some people lie on the Internet.

An important question to ask is what kind of lies are being told? Also, how big are those lies? Let's face it, on the Internet people lie about a lot of different things. Age and gender are two big ones. That hot teen girl your friend has been hitting on could very well be a 40-year-old man.

Watching out for predators on the Internet comes down to common sense and taking a few precautions:

- **Don't give out personal information.**

  This includes your full name, your home address, and your home phone number. Whether you're talking in an online forum, group chat room, or a new Facebook group, you still need to keep your personal information to yourself.

- **Don't participate in conversations that make you uncomfortable.**

  If the discussion turns to topics that make your skin crawl (or even itch), log off and stay off. Remember that the Internet, like the telephone, exists for

YOUR convenience. Just because people want to talk to you doesn't mean that you're obligated to talk to them. Most online communities provide ways to block access to specific members. If you're chatting with a new MySpace or Facebook friend who makes you uncomfortable, unfriend him. If you're using Instant Messenger, you can Block users you don't want to talk to. Even in email, you can add an address to your SPAM filters and have your email program automatically throw away any messages from that address.

- **NEVER tolerate harassment.**

  If those uncomfortable conversations start to feel like harassment, tell your parents and together, report that person to the authorities. They're not something you ever have to put up with.

- **If someone you met online wants to meet you in person, let your parents know.**

  Meeting people in person that you've met online isn't always dark and evil. As we know from online dating services, some people really do find their soul mates that way. Maybe even your teacher. In 2008, New Oxford High School in Pennsylvania saw a rash of marriages among teachers who'd met their spouses on Match.com. Sometimes, people who meet online inspire each other to serve others. A few years ago, a Gettysburg daycare operator named Paula was inspired by a new online friend to begin a local chapter of Project Linus, a charity that provides free homemade blankets to children in need of comforting. Members get together to make the blankets then distribute them to emergency rooms, homeless shelters, etc. This group was one of several that distributed blankets to children evacuated from the Katrina hurricane in 2005, then later the victims of the Haiti earthquake in 2010.

  Like Paula, your parents will have a much better idea than you will whether or not it's safe to meet someone you've met online. If nothing else, they'll be better prepared to verify the person's identity. Unlike many teens (who are often uncomfortable in new social situations), Paula felt no discomfort in phoning officials related to Project Linus to ask them about the woman she planned to meet.

If you're serious about meeting someone you "know" from online, be just as serious about verifying that person's identity in advance. If they claim to be active in a nearby town's church group, telephone the pastor and ask if that's true. For fellow scouts, check with the leader of their claimed troop. There are lots of ways to verify that someone is really who he says he is. Your parents can be very helpful in this.

- **Absolutely NEVER, EVER meet anyone F2F for the first time by yourself.**

  This is pretty self-explanatory but probably the most critical deterrent to online creeps. Don't put yourself in a dangerous situation when you don't need to.

12.2 Liars, Creeps, and Cyberstalkers

Most teenagers have no fear when it comes to the Internet. That's a good thing. Being afraid of the Internet would be like being afraid to walk to school, to the mall, or to a friend's house. You can't live in fear. At the same time, you need to be aware of your surroundings, protect yourself, and make the right choices in life. You must have the same awareness and make the right choices when you go online.

12.2.1 Liars

Most of us are taught from a very early age that it is simply unacceptable to lie. Yet we've been amazed at the number of tweens we know who've lied about their age to sign up for social networking sites. All of the major social networking sites, including MySpace and Facebook, require users to be at least 13. That's a safety precaution, recognizing that tweens often don't have the social skills and experience to protect themselves against online pretenders.

By lying about their ages to join social networking sites, those tweens become pretenders themselves. That's something to think about when assessing potential online friends. Is that potential Friend really 14 like it says in his profile? Maybe. But he could just as easily be 11 or 47. There's no way to tell. If your own birth date isn't quite what you claimed, what makes you think that anyone else's is?

12.2.2 Creeps

Because online forums and social networking sites allow people who may be total strangers at first to talk repeatedly and really get to know each other, they pose a special risk to teen users. Sexual predators often spend time on websites they know that teens frequent in order to establish friendships with teenagers. They try to strengthen relationships by being friendly and sympathetic, and sometimes by offering gifts. Eventually, those gifts come with an illicit price. Some reports claim that nearly 20% of kids aged 10 to 17 have been propositioned online at least once. Pedophiles rely on the anonymity of cyberspace as well as the naivety of younger web surfers.

Got a Creep to Report?

The FBI wants to know. Seriously!

Go to: www.fbi.gov and click on **Report Internet Crime**.

How serious is the problem of sexual predators online? That depends on who you ask. As far back as 2003, Microsoft shut down unsupervised Internet chat rooms in 28 countries, including much of Europe, Africa, Asia, Latin America, and the Middle East. They claimed that the chat rooms, "had become a haven for peddlers of junk email and sex predators." The American chat rooms were kept alive, but access was restricted to MSN subscribers—people for whom Microsoft had identification and billing information.

Sadly, Internet predators aren't limited to international chat rooms. Just ask the agents at Operation Blue-Ridge Thunder. Started in 1997 in a small Virginia town, this task force is dedicated to finding sexual predators online. Agents in the task force frequent chat rooms and online forums posing as young teens. Within two minutes of being online on a single day as a 13-year-old girl, Officer Rodney Thompson claims to have been approached by nine older men. Since 1997, the task force has provided law enforcement officers with leads on over 2,500 potential pedophiles. Even scarier, there are 46 similar task forces operating in other areas of the country.

Luckily, most predators use a pretty standard approach. If you know how these creeps operate, you can avoid them. Furthermore, if you run into problems, you can report them.

You should also remember that not all creeps are old perverts. When 16-year-old Celia received a message from an online friend that contained threats against his classmates, she didn't just log off. She printed out the message and took it to the police. The 17-year-old creep found his comments made public and himself under arrest. When police searched the chatter's home, they found weapons and disturbing Nazi paraphernalia. More often, it's the case that teens just rant, making silly threats they never intend to carry through. Still, making threats online, even if you don't really mean it, is just as dangerous as sending written threats in the mail. It's also every bit as illegal.

12.2.3 Cyberstalkers

In addition to general creeps and perverts, the Internet is also home to a very small but scary number of people who've been dubbed **cyberstalkers**.

Cyberstalker A predator who uses the Internet (via chat rooms, IM, or email) to harass his victim.

Cyberstalking is a high-tech form of general stalking. In cyberstalking, the stalker uses online forums such as gaming forums, social networking sites, and email to harass his victim. Stalking is more common than you probably think. Some experts claim that up to 5% of adults will be stalked at some point in their lifetime. With cyberstalking, the danger isn't always what the predator says TO you, it's also what the predator says ABOUT you. In recent cases, cyberstalkers have posted personal information (including address and phone number) to public forums along with malicious lies intended to damage the victim's reputation. False claims of drug use and promiscuity are common. Even ignoring the libel (slander is spoken), just being repeatedly contacted and harassed by someone you don't want to talk to is disturbing enough.

If you feel you are being stalked, it's important to report it to the police. Keep in mind that this applies to actual stalking. There are real differences between someone who is trying to engage you in bizarre conversation and someone who is stalking and threatening you. You can simply disengage from people who annoy you. Someone who is stalking or threatening you, *needs* to be reported to law enforcement officers. You know the difference.

Don't be afraid to report bad things. The FBI takes online abuse seriously.

12.3 Internet Monitoring

Your parents may or may not be concerned about your online acquaintances. If they're not, it's probably because they don't realize how connected you are. A lot of parents overlook the fact that home computers are far from the only access kids have to the Internet. A few years ago, Internet access was quite limited. Today, teens can choose between home PCs, friends' computers, school labs, libraries, and Internet cafes. State rest areas and even campgrounds now provide online access to tourists. As Lawrence Magid of the National Center for Missing and Exploited Children so accurately noted, "…children *don't* have to be in the company of responsible adults to use the Internet."

12.3.1 Monitoring Software

If your parents are concerned, they may have installed Internet monitoring software on your home computer. If they have, they had plenty of options to pick from—Parental Controls 2010, PC Tattletale, IAmBigBrother, Cyber Patrol, Safe Eyes, Net Nanny, and so on. Your parents could keep tabs on your Internet usage for as low $29.99. Not ***your*** parents? Don't be so sure. With that many products on the market, obviously somebody's parents are buying!

All Eyes On You?

If you're already concerned that your parents might be monitoring and have opted to use a friend's home computer instead, you may want to consider that *his* parents might be monitoring as well.

If you've become so entrenched in your online identity that you're willing to do or say things that you'd never do in person, you need to think about who and what you're becoming. Maybe it is time for you to put the keyboard down for a while and focus on what is important in your life. Your grades, your family, friendships that count, and your future.

12.3.2 Free Email Accounts

One method that teens often use to circumvent parental monitoring is collecting **free email accounts**. These are free web-based email accounts, unconnected to your Internet service provider, and accessible from any computer with Internet access. The major services are provided by Yahoo! (Yahoo! Mail), Microsoft (Windows Live Hotmail), and Google (Gmail).

Of course, teens aren't the only ones using free accounts. As early as 2008, Windows Live Hotmail had surpassed 270 million accounts. Granted, some of those accounts may have been dormant (opened by users who then forgot their passwords or simply never bothered to use the accounts). Still, the number of actual users for freebie accounts is pretty substantial.

Free email account A web-based email account you can access from anywhere and that isn't tied to your Internet Service Provider (ISP).

Another reason to use a free account is to keep SPAM away from your "real" email. Many online services require that you provide a valid email address. Having a freebie account is useful for all those times when you're required to provide a valid email address, and you don't really want the junk email that often follows (even when you uncheck the box that says "Yes, please send me additional offers and information!"). Using a free account lets you route that SPAM away from the important email in your ISP account. Because they are so overwhelmed by SPAM for millions of users, free account providers also do a fairly good job of killing the SPAM routed there. There are several advantages to this. Because the free accounts are web-based services, you're not wasting bandwidth or time downloading messages that you're only going to delete. Also, the free services spend a lot of time and effort keeping their SPAM filters up to date with the latest tricks the spammers are using. Identifying all those key words, etc. to define as filters in your own email program (like Outlook) would take you an awful lot of time. Yahoo! mail claims to identify 95% of SPAM messages which it immediately dumps into a Bulk email folder that users can delete sight unseen.

Using free accounts to avoid SPAM or check email from summer camp can be useful. That's not true about using free accounts to avoid Internet monitoring. Obviously, it's easy to create accounts on friends' systems and have free accounts on the Internet so your parents don't monitor you. But if you're going around the controls in your home to get to the Internet, you need to ask yourself some tough questions about why you are doing that in the first place.

Regardless of whether you use a free email account or your home email, you need to remember that communicating over the Internet is not secure. That racy email you deleted from your Sent folder could live on sitting on your email provider's

web server for years after you've forgotten what you said or why you said it. Even web pages that have been deleted eons ago still exist on backup tapes and search engine archives. Electronic data never really goes away. It just becomes a little bit harder to find. For this reason, you should NEVER write an email, send an instant message, or transmit a picture over the Internet that you wouldn't want your mother to see. Truthfully, you shouldn't say or post anything online that you wouldn't mind seeing on the front page of the *Wall Street Journal* or the *National Enquirer*!

12.4 Piracy on the Information Superhighway

If you think that the age of piracy ended shortly after the age of chivalry, think again. Just ask the Recording Industry Association of America. On their website, RIAA points out that, "Today's pirates operate not on the high seas but on the Internet, in illegal CD factories, distribution centers, and on the street." And the major steals lately seem concentrated on the Internet.

12.4.1 Are You a Pirate?

Pirates don't always manufacture thousands of fake CDs in third world countries. Sometimes, they download one song or one movie at a time for their own use. There's a public perception that making copies for yourself that you don't plan to sell doesn't really make you a pirate. That's not how the entertainment industry sees it. If you're downloading copyright protected songs or videos online, you may very well be a pirate. If you're using that new DVD burner to copy all your friends' personal video libraries, you're definitely a pirate!

Recently, 14-year-old Mark from San Francisco asked, "Why should I pay for music when I can get it for free?" Part of this answer is that it's just the right thing to do. It's also the properly legal thing to do.

Gram?!!!

Teens are clearly a big part of the Digital generation but hardly the only part. By 2009, a full 38% of senior citizens were using the Internet. A new Friend you can't quite place might not be another classmate—it might be your grandmother!

That's something to think about when you're tempted to post something that you'd NEVER bring up at the Thanksgiving dinner table.

The Right Stuff

Let's imagine that you and your buddies are starting a new band. It could be heavy metal, pop rock, rap, country western—whatever you are great at. Your guitar player Jamie even has a special "in" for you. His father produces music for a living.

Not long after you begin, your garage band takes off. Soon afterwards, Jamie's dad helps you to cut your very first commercial CD. This is great! You've accomplished what every grunge band in history merely dreams of—you get a hit song out of the gate and begin to receive royalties. Incredible luck, right? Only partly. You also put a TON of work into that success. You and your band practiced six days a week, not just one. You worked your guts out nailing down the right lyrics.

Now imagine that your CD is showing up on all those "free" music download sites. Everybody's listening to your work, but nobody's actually paying you. How would you feel? It wouldn't be right, would it?

The Legal Stuff

If the music being stolen from the Net were personally yours, you'd probably be pretty upset. You might even begin prosecuting anyone you caught in the act of stealing it. This pretty much sums up how the music industry feels. They've gotten very tired of seeing their profits downloaded away and they've begun to demand that the courts hold anyone they catch accountable.

The key word here is ANYONE. Obviously, the music industry sets their sights highest on shutting down the major pirating factories abroad. But they're also going after the little guys at home. And those little guys include teenagers.

12.4.2 Are You Putting Your Parents at Risk?

Music lovers used to have an all-or-nothing deal when it came to new releases. When we were teens, we often had to buy an entire new album when all we really wanted was one song. It is great to be able to purchase a single song instead of a whole CD, or to be able to download just a few songs and store them on an iPod. It probably seems even better when those few songs are "free."

In real life, however, few things are truly free. Downloading music without paying for it is not one of those things. It is stealing from the recording artists. That's the law, and the Recording Industry Association of America (RIAA) and the Motion

Picture Association of America (MPAA) are losing patience with the practice. No wonder. By 2007, the MPAA estimated that its members lost $3.8 billion a year due to Internet piracy.

In the past, people thought that it was only a crime if you made a copy you were planning to sell. With easy downloads, however, the practice of making personal copies has become so common that it's costing the entertainment industry a fortune. For years now, music sales and profits have either dropped or remained flat—an effect many blame on the pervasiveness of online piracy. When profits suffer, so do jobs. A 2007 study by the Institute for Policy Innovation found that overall piracy costs American workers 373,375 jobs and $16.3 billion in lost earnings per year. If you're thinking that doesn't affect you, consider that the annual income tax, sales tax, and corporate taxes on those profits would have been around $2.6 billion. When governments lose tax revenues due to piracy, that money is made up in higher taxes on honest people, like your parents.

Most Stolen Items

The "hottest" products being illegally downloaded from the Net:

- Music
- Movies
- Software
- Video games

To project jobs and profits, the big boys in the entertainment industry have started going after the little guys in a big way. One of their first targets was 12-year-old Brianna LaHara. Living in a Housing Authority apartment, Brianna hardly represented a major piracy ring. Like most young teens, she downloaded music only for her own use.

The press had a field day with the lawsuit, as did Congress. During later Senate Judiciary Hearings addressing music piracy, one senator sarcastically asked the RIAA president, "Are you headed to junior high schools to round up the usual suspects?" In the end though, the RIAA had the law on its side because downloading or simply making copyrighted material available for download without the permission of the owner is illegal. While she avoided the major fines she could have faced, Brianna's exploits cost her a $2,000 fine. Just imagine how many legal CDs she could have bought with that money.

Brianna is far from the only kid targeted. In 2005, Patti Santangelo of Wappinger Falls, NY was shocked at being sued by the music industry for piracy. She took her case to the media, pleading on national television that she didn't even know *how* to download music. The industry dropped the case, then turned around and sued two of Patti's five children. When a settlement was finally reached in 2009, neither side was talking numbers. But we'd bet that Ms. Santangelo wasn't happy with her kids' online piracy.

Pirating music may seem thrifty in the short term, but it can cost you and your parents big money if you're caught. While most settlements in early cases ranged from $2,000 to $7,500, American copyright law actually allows for damages of up to $150,000 per song. Before you download your next mix, you might consider whether your "free" CD is worth risking your parents' house. The RIAA and MPAA are actively looking for abusers. Don't give them an easy target.

Even if you're not putting your parents at legal risk by your downloading activities, you could still be putting their data at risk. As we discussed earlier, downloading "freebies" from peer to peer networks also brings a major risk of downloading spyware, adware, and other malware. Why risk the integrity of your computer or the money your parents have stashed in your college fund? It's not worth it.

Chapter 13

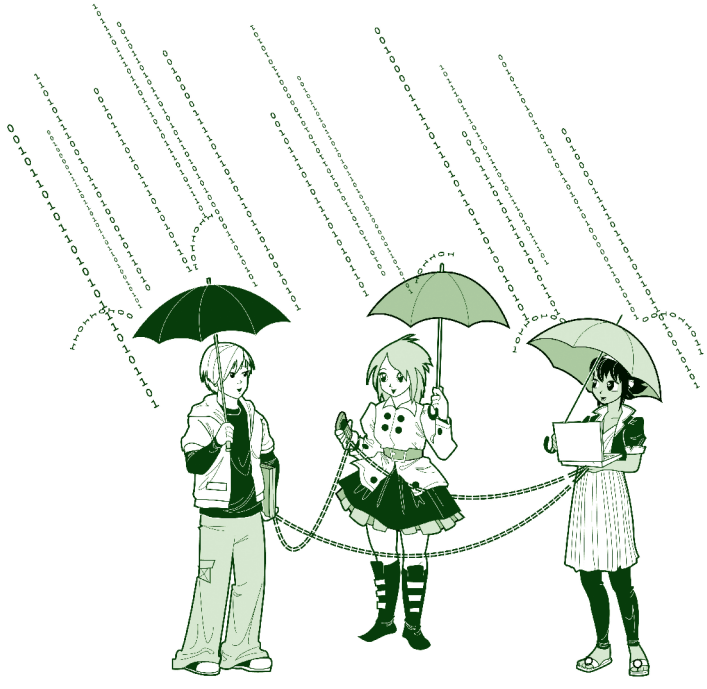
Any Port in a Storm

It was Friday evening, prime time for playing rounds of online games with friends from school. Douglas, a 15-year-old boy from Novato, California, had—as usual—gone straight from the dinner table to the Net.

Douglas is a serious gamer. He has every game system on the market. He even has two Microsoft Xbox 360s, a Sony Playstation 3, and a Nintendo Wii in his bedroom. Needless to say, he also spends time playing his favorite game, *World of Warcraft*, on the Internet. In the middle of the game, he lost his connection and was dropped from the gaming site. The following message flashed across his computer screen.

```
Connection Lost Out of
Bandwidth!!!
```

Douglas was annoyed that he couldn't finish his game and had no clue what that message meant. He started to wonder if he'd been dropped off because of the firewall on his parents' network. Douglas turned off the firewall, entered the gaming site and began to play his favorite game again. No drop off this time. Douglas decided to leave the firewall off while he was playing his game on the Internet.



While turning off the firewall sounded like a good idea to Douglas, that wasn't the problem. In fact, that created a *new* problem because turning off the firewall opened the door to his parents' home network to hackers. The bandwidth problem had to do with the network in Douglas's house. He really didn't have enough bandwidth coming into his house in the first place. In this chapter, you will see how you can test your bandwidth for free. Also, this chapter talks about some of the basics of networking and why firewalls are a critical component of security.

13.1 So What's a Network?

A computer network is a group of computers that are connected. Sometimes this is a physical connection using wires, cables, telephone lines or some combination of the three. Sometimes, as with "hot spots" and wireless networks, there is no physical connection. In all cases, however, the computers within a network are connected in a way that allows their users to share resources like files and/or physical devices like printers.

At school, the school's network is what allows you to create your research papers in one computer lab but pick up your printout in another. This is also what allows your teacher to enter grades at the computer on her desk and pick up printouts of student progress reports in the teacher's lounge.

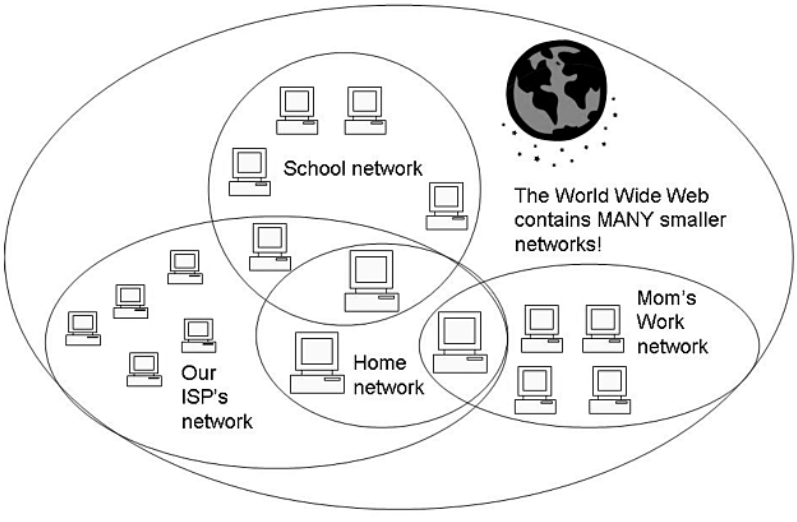
Computer networks have been around for a long time, and several technologies have been developed to enable computers to communicate. One of the most successful is a technology called **Ethernet**, invented by Bob Metcalfe in 1973.

Ethernet Ethernet lets computers on a Local Area Network (LAN), such as in an office building, connect to one another and to other network resources, such as servers.

Today's computer networks come in many shapes and sizes. They can be HUGE. A major university might have a computer network that connects thousands of students, faculty, and staff. A computer network can also be quite small. Consider the network at Douglas's house. That network connects just three computers—one for Douglas, one for his mom, and one for his dad. Because they're using network technology, the whole family can use the same Internet connection and send files to the same printer.

Regardless of their size, all networks work pretty much the same way and provide the same functions. That is, they all use one **protocol** or another to allow the computers and other devices in the network to talk to each other, and they all provide shared access to network resources. It's also possible for some resources in a network to be shared by some users but not others. This is why *you* can't send files to that printer in the teacher's lounge.

Protocol A protocol is a set of rules that computers use to communicate with each other.



The world is literally filled with computer networks!

One network can include all or part of another network. For example, the computer in your mom's home office is obviously part of your home network. However, it might also be connected to your mom's work network. It's also part of a network that includes all the machines that use the same **Internet Service Provider** (ISP). And, all of those machines are also part of the massive World Wide Web. So, we have networks inside networks inside other networks.

ISP Internet Service Provider. This is the company that provides the network that allows your computer to connect to the Internet.

13.2 How Networks Communicate—TCP/IP

Being part of a network is like being part of a community. In a community, life runs smoothly only when the people who form the community talk to each other. To share community resources, the members of the community need to communicate in ways that everyone can understand.

Computer networks are much the same. For computers to share resources, they need to communicate using a common language. In computer terms, that common language is called a protocol. A protocol is just a set of rules that computers use to communicate with each other.

TCP/IP is the protocol used most often to communicate on the Internet. TCP stands for transmission control protocol. When you "transmit" something, you are sending it somewhere. Thus, a "transmission" is whatever it is you are sending. So, TCP is the protocol that controls how things are transmitted on the Internet. In specifics, TCP works by sending data in blocks called packets. (When data is sent over the Internet, it is divided up into blocks of data called packets.) IP stands for Internet protocol and describes how computers send those data packets from one computer to another.

TCP/IP The protocol that most computers use to communicate on the Internet.

13.2.1 IP Addresses

For data packets to travel safely from one computer to another, the control protocol needs to know where the packets are going. It needs an IP address to send the packets to. It also needs to know the address the packets are coming from so that it can send a reply back to let the sender know that everything arrived safely.

Just like your house has a mailing address, every computer on the Internet has an IP address. Each IP address contains four groups of numbers separated by periods. For example, 192.168.1.1 is an IP address. Depending on what kind of Internet connection you have and how your ISP assigns addresses, you may have a static IP address or a dynamic IP address.

A static IP address is always exactly the same. Like your house address. That address is assigned when the house is built and it stays the same as long as the house is there. While your house address is assigned by the post office, your computer's IP address is assigned by your ISP, or possibly by indirectly connected machines if you have a private home network.

The advantage of having a static address for your house is that once a person learns your address, that person will always know your address. With IP addresses, this is a disadvantage. Once a hacker learns a static IP address, he would always know how to get back to that specific computer.

A dynamic IP address is issued when you connect to the Internet on any given day and you keep that address only until you log off the Internet or shut down your computer. The next time you connect to the Internet, you get a new (and probably different) IP address. Dynamic IP addresses help to protect you from being targeted repeatedly by a hacker trying to break into your computer. Your ISP assigns dynamic addresses from a pool of addresses available to that ISP. The protocol that manages the assignment of IP addresses is called **DHCP** (dynamic host configuration protocol).

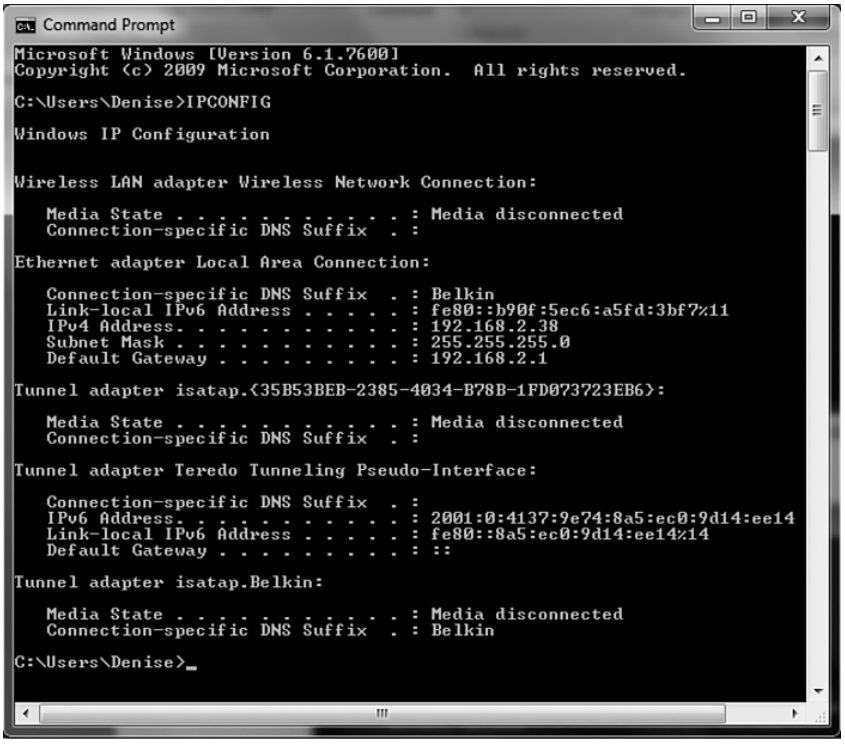
DHCP Dynamic host configuration protocol. DHCP is the protocol that an ISP uses to assign dynamic IP addresses.

Whether you have a static IP address or a dynamic IP address depends on two things: (1) what type of Internet connection you have, and (2) the policies of your ISP.

If your connection is always on, and you have a static IP address, attackers have a better chance of being successful at attacking you. It's simple to see that if you always have the same IP address you are easier to find. That does not mean that dynamic IP addresses are safe, however.

To find your IP address, first make sure that your computer is connected to the Internet. Now, click **Start > All Programs > Accessories > Command Prompt**. This will open a command prompt window.

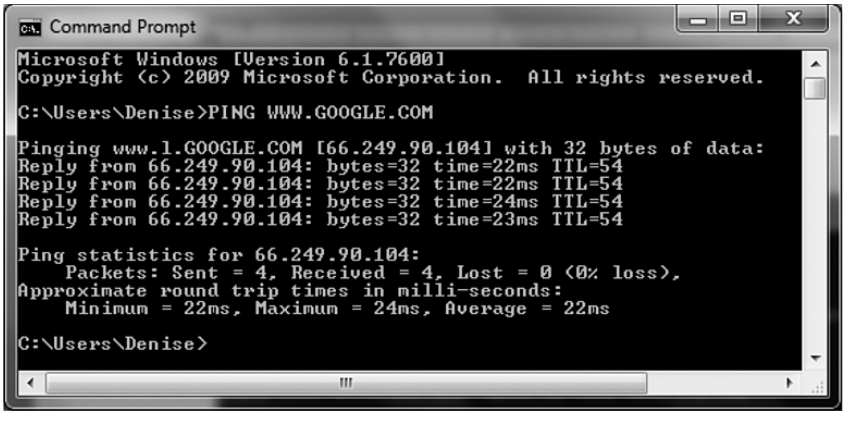
Enter the **ipconfig** command at end of the **C:\...>** prompt line. The window that displays next lists your IP address.



Now, shut down your computer and router and restart both of them. Connect to the Internet again and issue the **ipconfig** command a second time. If the address it returns matches the address it gave you the first time, you have a static IP address. If the two addresses don't match, you have a dynamic IP address.

You can also find the IP addresses for other computer systems by using the **ping** command. For example, to find the IP address for Google, click on **Start > All Programs > Accessories > Command Prompt** to again open a command prompt window. Then, enter the command **ping www.Google.com**.

The dialog box that displays next shows the IP address for www.Google.com under **Reply** from.



As we just pointed out, an IP address is similar to your home address. Once you have an address to a house, you can knock on the door and you might get in. When you find the IP address to a computer system, you've basically found the front door. To protect the front door to your network, you need several layers of defense including a firewall.

13.2.2 Data Packets

TCP/IP works by splitting messages and files being sent over the Internet into chunks called packets. Each packet contains part of the message or file plus the address of its destination.

In this type of communication, the computers sending data back and forth are called hosts. The computer sending the packet is the source host. The computer receiving the packet is the destination host. Both hosts use the same protocol to make sure that the packets arrive safely and in the right order.

Imagine that you were sending a book that you'd written from your computer to your teacher's computer. When you send the file containing the book, the controlling protocol would first split the book into smaller sections (packets). While actual data packets are considerably smaller, to make this simple let's imagine that each chapter becomes a packet. If there are six chapters in your book, there would be six data packets. Each packet would contain a separate chapter plus the IP address of your teacher's computer.

The control protocol would also add sequence information (say, the chapter number) to make sure that when the packets are assembled back into a single file at your teacher's computer, the chapters are still in the correct order. This makes sure that Chapter 1 comes first, Chapter 2 second, etc. To make things even more reliable, the control protocol on your teacher's computer would send a confirmation back to your computer, letting it know that the packets arrived safely.

13.2.3 Confirmation

There are actually a number of protocols that computers could use to communicate. TCP/IP is simply the most common. Some communications use a different protocol called UDP instead. Most Internet connections, however, use TCP/IP because it's considered to be more reliable.

TCP is considered more reliable because with TCP the computer sending the data receives confirmation that the data was actually received. UDP doesn't send confirmations. This makes UDP faster than TCP but not quite as reliable. In some cases, that's OK. Knowing that something actually made it to the destination is important for some programs, and not for others.

13.3 Port of Call

Where an IP address identifies the general location of your computer, the specific locations through which data actually gets into your computer are called ports. You can think of a port as a door into your computer. Unlike your house, which

probably has only two or three external doors, your computer has 65,535 ports. Some of these ports are allocated to specific applications. For example, AOL Instant Messenger uses port 5190. HTTP, the protocol used to communicate on web pages, runs on port 80 and port 8080.

When we say that an application runs on a specific port, what we really mean is that the application uses a service program to monitor that port. Thus, IM runs a service that hangs out at port 5190. It listens at that port for communications to arrive and responds when it detects those communications. You can think of these services as doormen. They wait at the door to see who knocks. When someone does knock (that is, data arrives at that port), the doormen (services) follow the rules (protocol) they've been given to decide whether or not to let the knockers in.

Attackers routinely scan the Internet looking for computers with open (unprotected) ports. This is called **port knocking**. To protect your computer and its data, you need to make sure that your ports are protected.

Port knocking Scanning the Internet looking for computers with open ports.

As you learned earlier, some applications run on specific ports. Of course, there are 65,535 available ports. You can specify access for services on specific ports through your firewall. Your firewall functions as a bouncer at an exclusive club—it has a "guest list" of exactly who is allowed in at which port. Thus, firewalls block access to ports that are not being used for specific applications. A firewall that is configured correctly won't accept connections to ports unless it's specifically told to do so. To protect your computer and its data, you need to make sure that your ports are protected. The list of ports and services is too extensive to cover here. You should visit your firewall vendor's site to see what ports and services are recommended and which ones are considered risky. Another good place to learn about ports and services is www.grc.com.

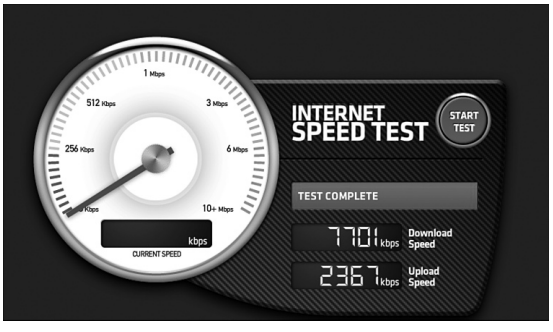
While you're still learning about firewalls, a simple step that you can take to protect your computer is to simply turn off your computer and router when you're not using them. Think about it. Hackers know that many home users leave their systems turned on and connected to the Internet for convenience. Therefore, it makes sense to turn off your computer and router when you are not connected to the Internet.

13.4 A Bit More about Bandwidth

Bandwidth is the speed at which data is sent over a communication line. Bandwidth measures how quickly your PC communicates with the Internet. Our gamer Douglas was dropped from the game he was playing over the Internet when the message *You are out of bandwidth* flashed across the screen. Like most users, Douglas never wondered how much bandwidth he had until he ran out. Do you know how much bandwidth you have?

After Douglas ran into the bandwidth error, his mom checked her cable bill and the website for her cable Internet service. She was paying for a bandwidth of 3 megabits per second. But when she checked the actual bandwidth she was getting, it turned out that only 1.7 megabits was available. She was paying for more than she was getting. When she complained to her ISP, they immediately coughed up the extra bandwidth.

If you're worried about a similar problem, there are a number of places on the Internet where you can run a bandwidth test on your system for free. One safe site is www.bandwidthplace.com.



Your potential bandwidth will depend on the type of Internet connection that you have.

13.5 Rings of Fire

When you started reading this book, you probably had no idea you had 65,535 available ports on your computer. Watching and blocking all those doors to your computer is one of the most important security jobs you need to fill. We've already

talked about a number of products and techniques you can use to protect your computer. A firewall is *one more* important layer of defense.

While you absolutely NEED a firewall, it is only *one* piece of the security protection puzzle. Using a firewall does **NOT** eliminate your need for other security products such as antivirus and anti-spyware programs unless your firewall comes as part of a bundled security solution. (Some security products aim to provide a total or near-total "solution" to security problems by bundling a whole bunch of different types of protective software into a single product.)

Firewalls do protect against hackers

An "intrusion" occurs when an attacker takes over your computer system. Many different techniques are used to hijack systems this way. Hackers might break into your system to leisurely poke around your files and read personal data; they might use your resources, launch a denial of service (DoS) attack, or steal your personal or financial information. Firewalls can help to protect you against many of these attacks by keeping you aware of when an outside program tries to access your computer through its ports or a when program running on your computer tries to access the Internet.

What Firewalls Can and Can't Do

Firewalls can protect against hackers and enforce security policies. But they can't make you behave and they don't protect against embedded attacks.

Firewalls do enforce security policies

Firewalls also enforce security policies to provide protection from inside out. The library has a firewall. Your school has a firewall. Even corporations have firewalls. In each case, the firewall has probably been set to block access to certain sites. Your school doesn't want you to visit sites with inappropriate or obscene material that your parents might object to. Your library has probably blocked access to free email accounts. Many libraries do this so that the computers intended to allow patrons to complete Internet research aren't always filled with people checking their email.

In all these cases, the firewall's actions represent a policy that was established for a reason. If you're behind a firewall and decide to try to figure out "a way around

it," you know that you really shouldn't be doing that. What you might not know is that what you are doing might be logged by the firewall.

Firewalls don't make you behave

You already know that just because a babysitter comes over doesn't mean kids will behave. They may not jump out the windows, but that's not to say they won't play *Guitar Hero* 'til the wee morning hours. Like a babysitter, a firewall only has so much control. A good firewall will enforce the security policies it's been set to enforce. Usually, that means that it might block certain sites or prevent certain programs from accessing the Internet. What it won't and can't do is make YOU behave online. Your firewall has no say over what you type when IMing your friends, which sites you visit (unless they're specifically blocked), or what kinds of email you send. Those things, along with the rest of your online behavior, are the products of your choices, not your firewall.

> "Firewalls are not in place to make you behave."
>
> —Marcus Ranum, inventor of the first firewall and the security expert who connected the White House to the Internet.

Firewalls don't protect against embedded attacks

Firewalls also don't protect you against "data-driven attacks." These types of attacks are initiated by an attack tool or malware that you inadvertently download or receive as an unwanted email attachment. When these attacks come in the form of malware that's downloaded without your knowledge or permission, they are sometimes called drive-by downloads. For more details on avoiding drive-by downloads, please read ***Chapter 3, Nasty "ware."***

13.5.1 So What's a Firewall?

A **firewall** is a piece of software that protects your computer (or your entire home network) by controlling the type of traffic that's allowed to pass between networks. In many ways, your firewall is like the lock on the front door to your house. Your front door lock keeps thieves, potential attackers, and nosy neighbors out of your house. By monitoring traffic to and from your computer and watching programs that communicate with your computer, your firewall performs much the same functions. It functions as the lock on your computer's front door to the

Internet, either permitting or denying program requests to send data into or out of your computer or network.

Firewall A piece of software that controls the type of traffic that is allowed to pass between networks.

Amazingly, many people don't know whether they're using a firewall. Some users actually have a firewall and don't even know it. If your home computer is networked, you may already have a firewall included in your router. A **router** is the physical device that routes information between devices within a network.

The major function of a firewall is to control traffic coming from or going to the Internet. Let's go back to Douglas's house. On his network, a Comcast cable modem is connected to a Linksys router. The family computers then connect to the Internet through that Linksys router. From the Internet, the only device that can be seen is the router. The family computers are "hiding behind" that router. The router passes along (i.e. "routes") all information going to and from the Internet. In no way can information get to or from any computer in Douglas's house without passing through the router.

Because a router protects the machines it routes data to, the router functions like a grand entrance way. That makes it a logical position for a firewall.

Router The physical device that routes information between devices within a network.

Of course, the router is not the ONLY place you'll want a firewall. You should also have a "personal" firewall on the PC itself. The personal firewall will allow you to monitor the applications running on your computer and restrict when and if those programs are allowed to send data to or from your computer. Using a personal firewall also provides a second layer of protection just in case a hacker compromises the firewall on your router. With only the router firewall, a hacker who compromises the router firewall can easily access any computers connected to that router. Add a personal firewall and that hacker has only made his way through your first line of defense.

13.5.2 Network Address Translation

For your first layer of defense, you need to have a firewall at the point where the Internet connects to your computer—that connection point is at your router. Another feature that is important is Network Address Translation (NAT). NAT allows you to use different IP addresses externally than you use internally. This helps to conceal your internal network, letting your home computer(s) "hide" behind your router. We talked earlier in this chapter about how your ISP assigns you an external IP address. A **NAT router** takes that assigned IP address and then distributes its own internal IP addresses to the computers inside your home network. From the Internet, only the router's address is visible. Because the NAT router assigns its own internal IP addresses, the IP address of each computer remains private.

Router Shopping List

- Network Address Translation
- Built-in firewall
- Wireless capability

NAT router A router that uses Network Address Translation to keep the IP address of your computer private and unviewable from the Internet.

Like operating systems and major application programs, routers also have known security holes. Therefore, you'll want to apply any patches or updates as needed. For most routers, you will also need to change the default login and password and make sure that the firmware is current.

13.5.3 So How Do Firewalls Protect Me?

Firewalls have two major protective functions:

- They permit or deny requests to send data to or from your computer.
- They monitor port access requests.

Permitting or Denying Data

There are two strategies you can choose from when setting up your firewall: a default permit strategy, or a default deny strategy.

- A *default permit* strategy means you configure the firewall to allow any host or protocol that you haven't specifically banned.

- A ***default deny*** strategy means that you list specific protocols and hosts that are allowed to pass through your firewall. Everything else is denied.

You'll notice that there's a world of difference between these two approaches. While default deny is a more censored and potentially robust approach, it's also a lot harder to configure. Unless you put a lot of work into your definitions, a default deny strategy could become so restrictive that your Internet connection might lose its utility. Default permit, of course, is much easier to configure—you basically block out known dangers, adding new blocks as new dangers are discovered. With default permit, you're allowing anything in until it's proven dangerous. With default deny, you're denying everything until it's proven safe.

Monitoring Port Access Requests

Firewalls monitor and regulate connections in and out of your computer by looking at everything that tries to access a port. You can configure your firewall to alert you every time an application or protocol tries to access a port.

Of course, ports that let data out can also let data in. Attackers often try to gain access to computer systems by first scanning for open ports. To protect your machine from port knocking, you need to configure your firewall to monitor and possibly block inbound connections. Attackers know that home users often don't install firewalls and frequently leave ports wide open—even ports on which vulnerable services are running. If you want to learn more about ports, services, and how firewalls work, a good place on the Internet is Steve Gibson's site, www.grc.com.

13.5.4 Firewall Settings

Techies can dig down into the heart of a firewall and block specific ports or applications. Most other users really prefer not to. Thankfully, most firewalls give you the flexibility to install quickly and easily by simply configuring your firewall setting to high, medium, or low. Which setting is best for you depends on what you do on the Internet.

We strongly suggest that you start by setting your firewall to High security. If you need to, you can adjust the level down from there to Medium. ("Low" security is rarely a wise idea.)

While you're setting up your firewall, don't forget about the logs. Firewall logs keep track of who and what tries to communicate with your system. It's nice to know who's poking around (or trying to peek) at your machine!

13.5.5 Free Firewalls

In recent years, firewalls have become more powerful, much more important, and—equally important to many users—fairly cheap. Better than cheap, some firewalls are actually free. You can get the free firewall Zone Alarm from www.zonelabs.com.

In or Out?

Windows Vista and Windows 7 firewalls block both inbound and outbound connections. The Windows XP firewall only blocks inbound connections.

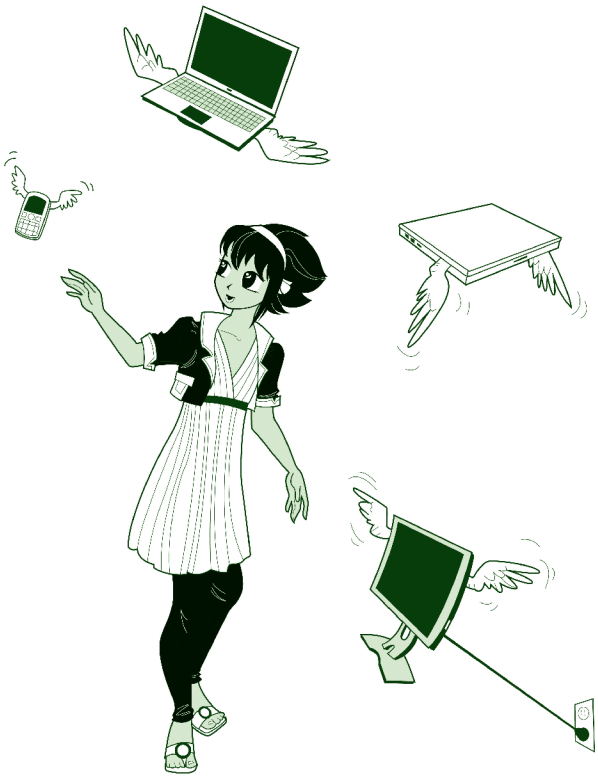
One frequently used firewall to beware of is the one built into Windows XP. That firewall only blocks inbound connections; it does nothing to block outgoing connections. Windows Vista and Windows 7 firewalls both fix that shortfall and block both inbound and outbound connections. To understand your firewall protection, make sure you know which OS your PC is running.

Chapter 14

Look Pa, No Strings!

Thirteen-year-old Michael was on cloud nine when he walked out of Best Buy with his new laptop; top speed, top features, great price, and—even better—already wireless enabled. Soon, he would become a wireless freeloader.

Before he even got home with it, Michael stopped at his friend Juan's house. Seconds after walking in the door, Michael was on the Net, courtesy of Juan's parents' wireless router. Same deal at his dad's house. Seconds through the door, pop open the laptop and straight to his favorite gaming site! Michael was an instant fan of wireless technology. Nothing, it seemed, could be easier.



Then Michael tried to connect to his stepmother's wireless network. No dice. Unlike his dad or Juan's parents, Michael's stepmom had taken the time to secure her wireless network. She'd set up a password, defined a network name, and enabled encryption. Michael was blocked. Right? Wrong. Michael hopped right onto the wireless network of a neighbor who was broadcasting to the entire neighborhood.

Michael's neighbors didn't complain, only because they didn't know. They were still sitting at home accessing their favorite sites, and completely unaware that the boy next door was literally stealing their Internet bandwidth. In less than two hours, Michael had gone from an overly excited new laptop owner to being just another **wireless freeloader**!

Wireless freeloader Someone who connects to an unsecured wireless connection that really belongs to someone else.

14.1 No More Strings

Perhaps you are one of the millions of people getting rid of all those computer cables tangled around your house? This is one reason why wireless home networks are popping up all over the world. They provide a simple clutter-free way to connect to the Internet from any room in your house—even your front deck or back yard. Connecting to the Internet wirelessly is the wave of the future. If you are not riding the wave now, you will be soon. Today, it's hard to buy a new laptop that *doesn't* come with wireless built in (using either a chip or a card).

The wireless capability on your PC still needs an access point, also known as a "hot spot," to connect to the Internet—you can't just connect to air. How secure your wireless network is likely to be, and how you go about making it more secure, depends to a large degree on what hardware you purchased and the capabilities within it and your PC. Your security level also depends on how (and whether) you configure those security features. Having security features is nice but in many cases you need to manually configure those features to actually use them.

14.2 What Is Wireless?

A traditional computer network uses physical wires, cables, and/or telephone lines to carry data between the physical devices (computers, printers, etc.) within the network. A **wireless network** uses radio waves instead. The wireless network card in your computer is essentially a two-way radio, also known as a transceiver, which can transmit and receive radio signals.

Wireless network A computer network that uses radio waves to send and receive data.

Wireless networks come in various shapes and sizes. There are mega-size wireless networks, including hundreds of square miles that provide wireless connections for major cities (these are different networks than the ones used by cell phones). A wireless network that size is called a wireless MAN, for Metropolitan Area Network. In most cases, however, when we discuss wireless networks, we are talking about **Wireless Local Area Networks (WLANs)** or even Wireless Personal Area Networks (WPANs). Since not many people use the term "PAN," those wireless personal in-house networks are also often called WLANs.

WLAN Wireless local area network.

A WLAN (of any size) works by using a radio transmission standard called Wi-Fi and the IEEE standard 802.11. Wi-Fi (pronounced Why-Fie!) stands for wireless fidelity. In really basic terms, when you are using a wireless network, your computer is sending and receiving data over radio waves in much the same way as a walkie-talkie. The major difference is that your run-of-the-mill toy store walkie-talkie is incredibly slow. Since most people speak fairly slowly, that's not a big deal for voice communications. For speed speakers, like auctioneers, that's not always true. Try speaking very quickly into a set of walkie-talkies. You'll find that the faster the speech, the harder it is to understand on the other end. Computers, of course, are seriously FAST speakers. They send and receive data at speeds much faster than even the auctioneer at Christie's auction house could match. To keep up with that speed, wireless networks use special **standard** ways to digitally code the data being sent to facilitate fast and crystal clear communications.

Standard A document that establishes uniform technical requirements to ensure that electronic devices can operate together.

IEEE, the Institute for Electrical and Electronics Engineers, is the international group that sets the standards used in most areas of communications. Their standards ensure that products made by different companies can still talk to each other. IEEE actually has several standards for Wi-Fi based wireless computer

networks. Those standards include 802.11b, 802.11g, 802.11a etc. You'll notice that there's a pattern here, in that all the Wi-Fi standards begin with 802.11. That's because IEEE uses a fairly complicated numbering system to "name" standards. That numbering system makes it hard to remember standard "names," but easy to see which standards are related to each other. The lowercase letter indicates the version of the standard. For example, 802.11b is version "b" of the 802.11 standard.

IEEE (Institute of Electrical and Electronics Engineers) The IEEE is a serious trendsetter, creating the standards for computer communications.

The Wi-Fi standards set the rules for how much data can be transmitted at a time, what speed that data is transmitted at, how far the radio signal travels, what radio spectrum is used, and how the communicating devices handle interference such as walls, hills, and devices like microwave ovens.

IEEE Standard	Distinction
802.11a	This standard provides only half the transmission range of 802.11b, but operates in the 5GHz radio spectrum which is less crowded.
802.11b	Devices using this standard transmit data at 11 megabits per second, and can send and receive data over a range of roughly 150 feet.
802.11g	Devices using this standard also send and receive data over a range of 150 feet, but can do so faster—at roughly 54 megabits per second.
801.11n	This standard improves upon the previous standards with several new features, including multiple-input multiple-output (MIMO).

In these (and other) areas, there are specific differences between the various 802.11 standards. Overall though, 802.11b and 802.11g are the most widely used in homes and hot spots, and b, g, and n are available in most Wi-Fi products.

When a wireless network is in operation, it creates what is usually called a **hot spot**. A hot spot is the area in which you can easily connect to the wireless network. If you're running a wireless network at home, your living room is most likely a hot spot.

Public places that offer wireless connections are also called hot spots. You are likely to find hot spots in most airports, many hotels, and nearly all Internet cafes.

Hot spot An area in which you can easily connect to a wireless network.

14.3 You Are Not Alone

If your home makes use of a wireless network, you are far from alone. Wireless connections are spreading quickly across most of the continental U.S. While visitors to Seattle may still gaze in awe at the Space Needle, they are probably unaware that at its top will soon be an antenna that beams Internet wireless capability over a 5-mile-square section of Seattle. How big can wireless networks be? Microsoft's new wireless network, begun in 2005, is projected to include upward of 17 *million* square feet. Among its many capabilities, this wireless network will allow up to 25,000 simultaneous sessions! That means that 25,000 people could use the network at the same time.

Of course, Microsoft rarely does anything in a small way. Still, wireless networks can be even larger. Australian ISP Unwired, in conjunction with Texas-based Navini, is building a **MAN**-size wireless network around Sydney covering 1,200 miles and including 3.5 million potential users. While you'd expect that kind of coverage in Australia's largest city, you probably wouldn't in America's rural farmland. Yet, farmers in Washington's Walla Walla County are actually part of an even larger wireless network—a 1,500 square-mile Wi-Fi hot spot. For scale, that's bigger than the entire state of Rhode Island!

Metropolitan Area Network (MAN) A wireless network that covers an area the size of a medium or large city.

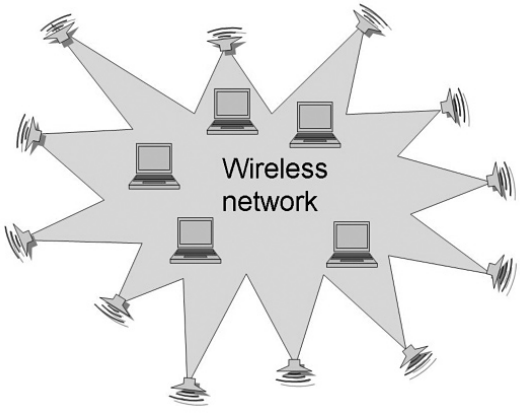
Because they are designed for easy access, wireless networks are especially vulnerable to attacks. By 2004, some analysts put the number of corporate Wi-Fi networks that had already been attacked by hackers at 30%. As Joe Kashi pointed out in the November 2005 edition of *Law Practice Today*, "Wireless hacking is so common that there are many websites and discussion groups devoted to the practice, from which the barely computer literate can download enough freeware

programs to overwhelm most small wireless networks." If anything the problem is worse, and there are even more sites and tools available today.

How exactly does that happen? Signals sent by your wireless device can be picked up by any device within your range. Hackers know this and some even drive around—literally, cruising the streets of commercial areas—searching for wireless networks. The computer literati call this **war driving**. Those war drivers are just waiting for their laptops to pick up a wireless network. This really isn't much different than our friend Michael, the 13-year-old freeloading on his neighbor's wireless. (Michael of course, didn't have to leave his living room, let alone drive around town. Which is pretty good given that he won't get his driver's permit for three more years…)

War driving A popular hacker past-time. This is literally driving around town trying to pick up wireless networks.

Wireless networks transmit data in every direction. Using the right tools, a savvy hacker can detect that data. If you're using a wireless network in your home, your data is also being scattered to the wind. Without proper security, any other computer with wireless capabilities in your range can connect to your access point, sometimes even unintentionally. Computers can detect nearby wireless networks automatically. This is a recent feature added to make it more convenient for users to connect to their local hot spots.



Wireless networks transmit data in EVERY direction!

As wireless networks proliferate, so does the number of wireless freeloaders. A wireless freeloader is a person who connects to someone else's wireless network without their permission—and usually without their knowledge. That connection might belong to an unsuspecting neighbor or to a nearby company with an unsecured access point.

It's even possible for a wireless freeloader to be unaware that they are freeloading. Wireless cards can be set to auto-connect (or "associate") to any available, unprotected network. If a person has this feature enabled, and their own network becomes unavailable, they may be unaware that their computer has re-connected to the Internet using someone else's Wi-Fi.

Michael, the 13-year-old wireless freeloader, exemplifies how easy it is to connect to a neighbor's network. Unless you've configured security on your wireless network, your neighbor just might be freeloading right now. We don't know about your neighbors, but some of ours are pretty nosy. We'd really rather not have them hitching a ride on the Internet through our networks. We don't want them snooping through our network traffic either. Our traffic is just that—ours.

14.4 Locking Down the WLAN

To avoid war drivers and keep freeloaders off of your wireless, there are several steps you need to take to lock down your wireless network:

1. Download the most recent firmware for your wireless router.
2. Change the router password and user name.
3. Change the default network name.
4. Enable encryption.

You'll notice that most of these steps involve changing the firmware or changing the settings (configuration) of the wireless **router**. The router is the physical device that creates your home network. Basically, it "routes" information to the right place within that network. In specific terms, that means that it forms the connection between your Internet connection (ISP) and the computers and devices within your home network. (With some wireless cards it's possible to create an "ad-hoc"

wireless network between two computers without using an access point, but this isn't recommended and doesn't provide the security or performance that using an access point does.)

Router The physical device that routes information between devices within a network.

In addition to connecting your computer(s) to the Internet, the router also connects them to each other. When information is "routed" it's being sent from one place to another, or more specifically, from one physical device to another. It's your router that sends information between your computer and the Internet or between your mom's computer in her home office and the photo printer in your living room. Just as the Post Office uses addresses and zip codes to deliver packages from one person to another, your data has "from" and "to" addresses that help it get from your computer to where you need it to go. In many ways, you can think of your router as the postal worker who uses the addresses on your data to make sure that it's delivered to the right device and program.

A traditional "wired" router moves your data by using physical cables and phone lines. Your wireless router instead routes information within your home using the radio frequencies defined by the Wi-Fi standard being used. It may still use a phone line or cable to communicate with your ISP. Or, it may not. If you're using a satellite-based ISP, your router may use radio frequencies to talk to your ISP as well as to communicate with the computers and other devices inside your home.

14.4.1 Downloading the Latest Firmware

You're no doubt already familiar with the terms hardware and software. Hardware is anything you can physically touch. This includes your computer itself, your printer, your digital camera, and CDs. Software is the instructions that tell the hardware what to do. Unlike hardware, which is pretty much molded when it's physically assembled, software is dynamic. It can change, and change fairly easily. Firmware is something in between hardware and software. Like software, firmware consists of computer programs that tell your computer what to do. Unlike traditional software, you cannot add and remove components to firmware easily. What this means is that you are limited to the functionality provided by the

firmware version which you are running. If you wish to enhance its functionality, typically you will have to upgrade to a whole new firmware rather than just installing a patch or adding a new component.

Firmware is embedded in the physical devices in your computer system. Part of your computer's firmware, called the *BIOS*, is what allows you to reboot so that you can reinstall software even if you've downloaded a virus that completely trashed your hard drive. Like your computer itself, the wireless router that creates and manages your wireless network also has its own firmware. Sometimes, hackers are able to get into systems like wireless networks because of security holes in the firmware or due to limitations of the security features in the firmware. Because of this, it's very important that your wireless router has the most current firmware installed. You need to check this, even if you're dealing with a brand new, just out of the box router. For all you know, that "new" router may have shipped late last year and sat on a shelf at your favorite electronics store for months. So, the firmware may be out of date and the hackers may have detected new security holes since that router was originally produced.

Always be sure to check your router's firmware and the vendor site to make sure you have the latest version. Simply go to the vendor's website and look for the most recent firmware for your device. This is most easy to do by searching for the router name and the phrase "firmware." To perform the actual upgrade, follow the instructions provided by the company that makes your router. It is important that you only download firmware from the original vendor's website. Do not install firmware from a third party—such as a free software download site or an Internet forum.

14.4.2 Changing the Router Password and User Name

Like many important physical devices, your wireless router comes with password protection. Obviously, you don't want just anyone to be able to change your router settings and define who's allowed to use your wireless network.

When your router arrives in its little box from the store, it will have a default user name and password already set. This is usually something pretty obvious, like user name **Administrator** or **Admin** and password **System**. Like you, anyone who's

ever seen this particular router or the installation instructions knows the default user name and password. Since you don't want just anyone changing your router settings, you need to change those defaults as soon as you unpack the router. For specific instructions, read the User's Guide that you should find inside the box your router came in, or online at the vendor's site.

Default Passwords and User Names...

are a hacker's easiest route into your router and the rest of your home network. Change them immediately!

Ideally, you should select complex words or phrases for your user name and password. Avoid using anything even remotely close to the default values. For your user name, also avoid using anything that's blindingly obvious. Your name, your favorite football team, the best online game you've ever played, and anything at all similar to the terms **Admin**, **Administrator**, or **System** are especially bad choices. For your password, follow the rules for selecting hard-to-break passwords that we discussed in ***Chapter 4, Hackers and Crackers***.

14.4.3 Changing the Default Network Name

Just as every computer on the web has a unique IP address, every wireless network can have a unique name. This name is called the Service Set Identifier or SSID. The SSID is a unique, 32-character name that identifies your wireless network and distinguishes it from nearby networks.

Because your wireless router can't actually route anything without a valid SSID, router manufacturers set a default value for this name. The default SSIDs of every access point model—along with the associated default user names and passwords—are available online. In some cases, the default name can help hackers identify access points with known security holes. To protect your network from unexpected visitors, you want to change that default value as soon as you set up the router. This should be your next step after you've changed the router's administrative user name and password. However, don't change it to something too revealing, like "Jim's home network," or worse, use your address in the name, "143 Broadway." There's no reason to reveal that much information.

For most operating systems, you will change the SSID as part of installing your wireless router, using the router's administration portal or configuration software—often accessible through a web browser. Consult the manual or manufacturer's instructions that came with your wireless router for specific instructions.

14.4.4 Enabling Encryption

When you enable encryption, you're telling the router to scramble your data to keep unauthorized snoopers from making sense of any data they intercept.

In ***Chapter 8, Safe Cyber Shopping***, we discussed the types of encryption used to protect online commerce. Different, but similar, types of encryption are used to protect data being broadcast in wireless networks.

For wireless networks, three types of encryption methods are possible, each using a different security protocol.

WEP	Wired Equivalent Privacy	This is an older standard, and it's useless to protect you against today's hackers. If this is the best option you have available, you should replace it *immediately*.
WPA	Wi-Fi Protected Access	This encryption method uses the Temporal Key Integrity Protocol (TKIP). While it is much better than WEP, it has some address security shortcomings that may leave your data at risk.
WPA2	Wi-Fi Protected Access 2	WPA2 uses the IEEE Advanced Encryption Standard (AES) security protocol. For today, this is your best bet for secure encryption. However, it does have some hardware limitations and may not work with some older devices.

Regardless of whether you opt for WPA or WPA2, you'll need to define a WPA-PSK. The PSK is a pre-shared key that is used to encrypt (and subsequently decrypt) data shared between your computer and the wireless access point (your router). To use encryption, you need to define that pre-shared key. For most routers, you will do that by providing a pass phrase that the router uses to generate the encryption key.

A good pass phrase, like a good password, should be hard to guess and include letters and numbers as well as special characters. You might start with a simple phrase like "Mary had a little lamb." Now, let's knock it up a notch by replacing

all the vowels with numbers. Let's change every letter "a" to "4," every letter "e" to "3," and every letter "i" to 1. To make it even more robust, now throw in some punctuation marks at the start and end of the phrase. The result:

```
Mary had a little lamb.
```

becomes:

```
"!*m4rry h4d 4 l1ttl3 l4mb!!*".
```

14.4.5 Other Steps

Many books recommend additional steps to secure a wireless network. These steps often include turning off SSID broadcasting and limiting allowed network addresses to specific MAC addresses (MAC filtering). Neither of these steps is necessary or recommended because they will do little or nothing to actually secure your network.

Even with the SSID turned off, your network is easily detected. Modern operating systems, like Windows 7, can detect the presence of a "hidden" wireless network. In addition, even the most inexperienced hacker can download simple (and free) tools to detect or "sniff" network traffic and detect hidden networks.

Likewise, using MAC filtering won't secure your network. In theory, by only allowing computers with specific MAC addresses to access your network (presumably only your computers) you should be able to prevent unauthorized persons from connecting. In reality, anyone can sniff network traffic and discover which MAC addresses are authorized. Using widely available software, they can then "spoof" an authorized MAC address. By *spoofing* they can masquerade as a computer that's allowed on your network by using its MAC address.

All that either one of these techniques does is attempt to hide your network. Neither technique will deter, or even stall, a determined attacker. What they will do is make managing your network more difficult, and make it less user-friendly for legitimate network users. Depending on your router and the amount of network traffic, MAC filtering may also slow your network down.

Other experts may argue that these techniques will prevent casual war-drivers or freeloaders from using your network, but that is exactly what encryption is for.

Once your network has been properly secured using the other techniques mentioned in this chapter, you needn't worry about hiding it.

14.5 Public Hot Spots

As wireless technology continues to drop in price and surge in popularity, public hot spots are popping up in cafes, hotels, airports, book stores, fast food restaurants and even in the air. Boeing is building aircraft with wireless access points. As of 2009, some airlines had already begun to offer in-flight Wi-Fi on selected routes. Imagine flying high with hot spots at 35,000 feet with Wi-Fi enabled laptops.

The big problem with public hot spots, however, is that for ease of use they don't enable encryption. This means that hackers or eavesdroppers can read your traffic, unless the websites you're accessing are using encryption (https://).

There are always dangers inherent in conducting private business in public hot spots. Because they are among the heaviest users of this technology, teens need to be especially aware of those dangers and take at least basic precautions to protect themselves.

Security Tips for Public Hot Spots

- **Be discreet.** Using your laptop in a hot spot is much like using your cell phone in the middle of a large restaurant. Your conversation might not be completely private. Don't send anything out over the wire that you wouldn't mind seeing on the front page of the *Wall Street Journal*.

Beware the Evil Twin...

Malicious hackers have used a technique called the Evil Twin to tap into wireless systems. The attackers set their SSID to match the SSID of a public hot spot or a company's wireless network. Then, they initiate a denial of service attack against the "real" network, effectively taking it offline. Legitimate users lose connection to that "real" network and unknowingly pick up the evil twin instead. Sometimes, this is called a "man in the middle" attack! In some cases, attackers don't even bother to copy the name and simply set up an access point nearby named "free Wi-Fi," or something similar, to entice people to connect.

- **Keep your files to yourself.** Turn off file sharing so that hackers can't access your files.
- **Be up-to-date.** Make sure you have the latest service packs and updates installed for your operating system (that automatically turns off file sharing and installs critical security patches).
- **Use VPN if you need to.** If you have sensitive data on your laptop, you should use a virtual private network (VPN) when you connect to any network, whether or not you're currently sitting in a hot spot.
- **Use sites that are SSL enabled.** Sending any private or sensitive information? Be sure the site in question is SSL enabled.

14.6 Mobile Devices

Laptop computers are no longer the only devices that people are using on wireless networks. You may in fact be accessing the Net on anything but your laptop—your PDA (Personal Digital Assistant), BlackBerry, iPhone, iPad, Droid, organizer, digital camera, and even older cell phones.

Some of the newer mobile devices even combine all of the above. Heavy travelers often rely on smart phones which provide a cell phone, digital camera (for picture capture), Web browser, email access, MP3 music player, social networks, and an organizer—all in a single device. While these devices provide the functionality of multiple pieces of equipment, they also provide all the vulnerabilities.

Bottling up malicious threats to your phone requires vigilance, common sense, and protective software!

14.6.1 Attacks on Mobile Devices

Hackers are now beginning to target mobile devices, particularly smart phones and PDAs. Smart phones are especially high targets because so few users think about Internet security when they think about their cell phones.

But they should. Some pretty nasty attacks have already been launched at the cell phone market. One such attack appeared as a Trojan hidden in the installer of a popular video game enticing users to download it to their phones. Once installed, the game released a worm called Cabir on the phone. Thankfully, Cabir was fairly benign—spreading itself to other phones but not causing much damage when it landed. It did, however, have the nasty side effect of eating up battery life, leaving cell users stranded with dead phones that should have still been charged.

At the Black Hat conference in July 2009, security researchers showed the audience how to break into iPhones by sending malicious code via SMS (text message) without the users knowing they had just been attacked. Although Apple quickly released a patch, an attack like this demonstrates just how quickly the bad guys look for flaws and create malware to exploit the flaws found.

Popular Mobile Operating Systems

- Apple iPhone
- BlackBerry
- Google Android
- Microsoft Windows Mobile

Like computers, which tend to use either Windows or Mac OS, mobile devices also make use of operating systems. To protect your mobile device from attack, you need to know which operating system it uses and how to protect it. In addition to relying on different operating systems than their larger laptop counterparts, mobile devices also tend to use different communications standards. Most of today's mobile devices use a technology called **Bluetooth** to access other wireless devices, such as printers and other phones. Most smart phones (iPhone, Android, BlackBerry, etc.) can easily connect to the Internet through Wi-Fi access points.

Bluetooth An open wireless protocol that allows data to be exchanged by mobile devices over short distances.

While mobile devices are certainly at risk from malicious code attacks, they are also at physical risk in a way that other wireless technology isn't. Given their size (and high expense), most users keep a strong physical hand on their laptop computers. Those same users don't always have a good hand on their mobiles. We've seen cell phones left behind at schools, cafes, and restaurants. Many a user has also had

Backing Up Your Mobile Devices?

Computer backups are an awful lot like dental floss. We all know what we should be doing, but most of us fall down (at least sporadically) in execution.

The next time you "suddenly remember" to back up your computer files, don't forget to back up your mobile device. Like your computer, it probably contains important data (address books, appointments, etc.) that you really wouldn't want to lose forever.

a cell phone slip out of her back pocket and find its way into a friend's sofa or under a car seat. Don't forget to back up your data just in case your phone slips away. Check with your vendor for backup software and instructions on backing up your device.

To protect yourself in the event that your mobile literally slips into an intruder's hands, you also need to set a hardy password to protect its contents. Don't make the same mistake as Paris Hilton. Never one to seriously protect her personal information, in 2004 Paris found that her PDA's address book and photos had been posted to the Internet by intruders who'd hacked into her T-Mobile account and were apparently reading her email as well. How'd they get her password? Like many users, Paris picked a weak password. In her case, she chose the name of her dog. Of course, any person who's ever followed her antics (on purpose or not), knew that Tinkerbell was near and dear to Miss Hilton's heart. Surely *you* can pick a more secure password!

14.6.2 Sexting

Sometimes, the worst damage isn't done by hackers or bad guys. It's self-inflected. This is certainly the case with **sexting**. Sexting is sending an obscene or heavily suggestive photo electronically. In theory, that includes inappropriate photos sent by email and instant messenger. In practice, when most people talk about sexting, they mean photos sent via cell phone.

Sexting Sending nude, semi-nude, or sexually explicit photos via text message or over the Internet.

Today Chloe had to leave her AP English class because the police wanted to scan her phone. You see, three months ago, Chloe sent a very inappropriate photo of herself to Kyle. Yesterday, when she broke up with him, Kyle forwarded that photo to everyone in his cell phone's address book. The police scanned Kyle's phone too, and the phones of his friends. Talk in the halls was that Kyle might be charged with distributing child pornography. He was planning to go from high school player to college scholarship. Now he might go from varsity basketball to Registered Sex Offender. At least his privates are still private. Chloe has no idea who's seen her photo. One of the rumors going around is that Kyle's friend Jon used his iPhone to upload Chloe's photo to an amateur porn site. She may never know. Even if she wanted to check, it would be impossible for her to track.

There are several major problems with sexting. The most obvious is that eventually, the kids sending those photos of themselves will be humiliated and wonder how they could have ever done something so obviously stupid.

Another problem with sexting is that authorities currently don't know how to treat it. Take the sad case above. Chloe and Kyle (obviously not their real names) are real kids currently attending high school in a small Pennsylvania town. Pennsylvania law—like that in the most of the United States—doesn't provide a clear path for prosecutors. Depending on the personal approach of the local prosecutor, one of three things could happen in this case:

- Chloe and Kyle could be officially "warned" and left to deal with their humiliation privately.
- Kyle could be charged with harassment.
- Kyle and Chloe could BOTH be charged with distributing child pornography.

If the last option is followed, both teens could be placed in foster care and/or juvenile detention. If convicted, both would be forever ineligible for college loans, college scholarships, military service, and many types of employment.

In this case, a crime of harassment clearly did occur when Kyle forwarded the photo. However, let's imagine that the photo was kept just between them. Under many state laws, Kyle and Chloe could be charged with distributing and receiving

child pornography EVEN if no one else sees the photos. And Kyle and Chloe would be far from alone.

Recent research suggests that up to 20% of teenagers have sent or received some form of sexual message. Is that stupid behavior? Absolutely. Is it deserving of a felony conviction? That depends on who you ask. Andy Hoover, legislative director for the Pennsylvania chapter of the American Civil Liberty Union (ACLU), comments that, "Kids are going to engage in irresponsible behavior. The best way to deal with that is through education, not giving them a criminal record." Of course, Hoover isn't a prosecutor and not all prosecutors agree with the ACLU's interpretation. One especially aggressive district attorney in Pennsylvania filed felony child pornography charges against two teen girls who photographed themselves wearing training bras at a pajama party. In fairness, he did offer to drop the felony charges if the girls agreed to take a series of classes he deemed appropriate, write essays explaining why being photographed in their bras was wrong, and agree to be placed on probation and submit to random drug tests. Their parents declined and appealed the case instead.

Even without the criminal considerations (which are some pretty major considerations), sexting creates major concerns for long-term privacy. Photos can migrate from phone to web in seconds leaving digital trails that last decades. Do you want to risk having sleazy teen photos surface when you're job hunting? Or how about when your kids are online 10 or 15 years from now researching family history for a school project?

Short-term privacy is also a consideration. We'd strongly recommend you follow the advice of 19-year-old Breena Aguila. "I wouldn't do it. I wouldn't trust a guy not to show somebody." Would you?

14.7 Wrapping It Up

Dispensing with wires is only the first step to going wireless in security and freedom. You also need to lock-down your new wireless to keep it safe. Changing passwords, downloading the most recent firmware, changing the default network name, and enabling encryption are necessary steps to cutting the strings. Even then, don't conduct financial transactions on unsecured wireless networks.

Remember that most public hot spots are not secure. Public hot spots are fine for browsing the Internet and email, but not for financial transactions.

Finally, you need to remember that not all wireless devices are created equal. Like your wireless network, your cell phones and PDAs also require security software attention. Most of all, you need to be aware of the dangers and remember them in deciding when and how to safely use your wireless technology:

- Think before you send any messages over your cell phone. Text messages are not always private.
- Don't use your phone to attack others. That's a form of cyberbullying.
- Don't put up with bullying texts from others. If someone is harassing you over your cell phone, keep a record of the messages and talk to your parents. You might need to get the authorities involved.
- Don't use your phone to access porn, or send naked photos of anyone (friend, foe, or stranger). You could be charged with distributing child pornography and end up as a registered sex offender.
- Don't forget that your friends have cameras in their phones too. They might take videos and pictures and post them to the web without your knowledge. If your friends are taking inappropriate photos or videos, walk away.

Chapter 15

Getting Help

Tim, a 16-year-old from Los Gatos, California, downloaded a write-your-own-virus toolkit off the Internet. Tim was getting into programming and, like most teens who write viruses, he was up for a new challenge.

With the do-it-yourself virus kit in hand, Tim was able to construct his own virus in record time. He didn't release it into the wild, of course. Becoming a black hat was never Tim's goal. He just wanted to know that he *could* do it if he wanted to. He wasn't really thinking like a bad guy.

That was actually the source of his downfall. If he had been thinking like a malicious hacker, it would have occurred to him that viruses are pretty nasty bits of code. While his hacker toolkit made it almost embarrassingly simple to create his malicious code, it didn't tell him squat about how to get rid of the new virus.

The end result? The would-be hacker completely trashed his own computer system. That's something to think about if you're tempted to try your hand at creating malicious code or even post a less-than-politic blog entry. On the Internet as well as in real life, you nearly always get what you give.

So far, every chapter in this book has started out with a teen security story. In addition to being true, most of these stories are about how easy it is to fall victim to hackers and malicious code if your PC isn't protected by the right security software.

Since Michelangelo and other famous viruses propelled the concept of protective software into the public view, the tools available to defend home computers have become awfully diverse and complicated. In the past, you could get away with just a firewall. Then you needed antivirus protection, then protection against SPAM, then anti-spyware, then intrusion detection, possibly web filtering, privacy and anti-fraud. The list gets longer each year. That's good for security vendors, but not so good if you have to buy licenses to run all of this software, and renew those licenses every year.

Before you purchase any security products, you need to understand which components are critical. Some security vendors offer bundled solutions—combining multiple products under one license. This is especially important if you have more than one computer to protect. As your home computing power grows (and it will), you'll want to simplify computer security. A good way to do that is to combine as many features as possible under one license. If the vendor you are using doesn't do that, find another vendor.

15.1 Security Essentials

There are essential security products (and downloads such as patches) that you MUST have in order to keep nasty code and unwanted visitors off your computer system. These essential features are

- **Patches**—To prevent problems before they happen.
- **Antivirus software**—To keep new viruses from infecting your machine.
- **Anti-adware and anti-spyware software**—To protect you from both spyware and adware.
- **Firewall protection**—To keep unwanted visitors at bay.
- **Backup software**—To keep your files available, just in case.

You'll notice that the first feature here is more a procedure than a product. That is, you don't so much buy patches as you either make it a habit to apply them or—even better—you configure your machine so that patches are applied automatically. Much of the malicious code that protective software wards off or removes can be avoided by making sure that any security holes in your operating system, application programs, and protective tools are patched as soon as those security holes are identified. For now, just keep in mind that applying patches is absolutely essential. Failing to do so can keep the rest of the tools we're about to discuss from working properly, or in some cases, even working at all.

The other items listed above form a category called "protective software." In a perfect world, you could run to Best Buy, walk to the aisle labeled "Protective Software" and pick up any one of a hundred perfect programs that would each meet every one of your computer protection needs.

Real life isn't that simple. Most protective software on the market includes two or more of the features listed above. Your mission is to find the right combination of products and procedures to perform all five. Because some vendors do bundle multiple security solutions under one license, you may be able to get all of these features in one product in a way that meets your needs. Keeping to one product makes things easier to administer at home. You have to decide, however, whether the features being bundled give you all the security you need. And, of course, you do often get what you pay for. The more robust and feature-packed packages are usually more expensive. Only you can determine what it's worth to protect your computer, your data, your privacy, and your identity.

15.2 Additional Niceties

The last section discusses the absolute necessities for security. There are also additional features that aren't quite necessary but may make your life much, much easier. These include:

- SPAM blocking/filtering

  An incredible amount of malicious code travels via unwanted, unsolicited email. Blocking SPAM reduces your exposure to this code. It also saves you a lot of wasted time and general annoyance. SPAM blocking is offered as a

feature on many packages designed to eliminate spyware as well as in some antivirus packages.

- SPIM blocking/filtering

  SPIM is the instant message version of SPAM. A first line of defense in blocking SPIM is turning on your "buddy list." You might also want a product for IM authentication and encryption, logging IM communications, and so on. Encryption is critical because anything you send out over IM goes out in the clear. So if you value your inheritance, don't use IM on the same computer your parents use for online banking! Also check that your antivirus software looks for malicious code in IM attachments.

- Anti-fraud, Privacy, and Identity protection

  Many computer security packages now include anti-fraud protection, privacy protection, and identity fraud protection. Identity fraud and privacy invasions are rapidly becoming the largest problems facing computer users. If the product that you're using doesn't protect you from these threats, you may want to consider switching vendors.

- Intrusion prevention

  Detecting attacks and potential intrusions used to be something that only large corporations really worried about. That was before home computer users found that their machines had been drafted to bot armies for coordinated denial of service (DoS) attacks. Most, but not all, firewalls include intrusion prevention.

- Email and file encryption

  Encryption is a double-edged sword. While it's useful in protecting your data, unless used carefully it can protect your data so well that even YOU can't read it. On the plus side, if you do opt to encrypt, some of the best tools are either free or included in your operating system. For email encryption, the gold standard is Pretty Good Privacy (PGP) from pgp.com. The downside is that PGP works only if the people you're sending email to also use it. Disk encryption is actually provided within Windows 7. Encrypt with care though. Some better options might be password protecting your files and always

keeping in mind that anything you send out over email could easily become public knowledge. Send only emails that you wouldn't mind reading as headlines in the *New York Times*.

- Pop-up blockers

  Several of the nastier versions of adware circulating in 2010 made the rounds by masquerading as free spyware checkers. While these versions had little in common (they were made by different companies and even originated in different countries) what they all shared was that they nabbed users by showing up as pop-up windows. Having read this far into the book, you are no doubt MUCH too security-savvy to fall for this particular trick. However, if you share a computer with a younger sibling or less security conscious classmates, you could easily fall victim to this ruse. Blocking pop-ups is a great way to eliminate that risk.

15.3 Bundled Security Solutions

Although it's unlikely that you'll find a single product that meets all of your computer security needs, you still might consider purchasing a bundled approach. At the very least, make sure that the solution you buy includes more than just antivirus protection.

Buying a bundled approach has a number of advantages. First, every security product you buy has a license. When that product is upgraded, you need to purchase the upgrade. This has a number of financial repercussions. Obviously, if you buy four separate programs to protect your machine, you're paying for four different licenses. Even if you pick up your protective software as "freeware," you're still investing time and energy to evaluate, select, download, and install those four packages. Where this becomes even more cumbersome, and potentially expensive, is when you start looking at upgrades for all four of those products as well. In addition to the expense of paying for separate upgrades, you're also hit with the time factor of continually applying updates. With four vendors, it's unlikely that upgrades will be offered at the same time. You could be renewing your virus

protection in January, renewing your firewall in February, renewing your spyware protection in March, etc. From a time perspective, this is simply too much work—especially if you have multiple computers in your house. To function properly, computer security needs to become second nature. It should not become a second job!

Bundled packages can be especially cost-effective for multi-computer households. Most of the top-rated bundled packages are available in home versions that support three to six computers.

If you're concerned about the price of protecting even one home computer, relax. You can find many excellent security packages for free on the Internet. The trick is to make sure you download that free software from reputable sites. You don't want to end up downloading a Trojan by mistake. This is why it's so important for you to know which vendor sites are trustworthy.

Another factor to consider when using multiple products for computer protection is that not all of the products work and play well together. In particular, you shouldn't run multiple versions of firewalls and you *can't* run two different versions of antivirus software.

15.4 Backup Products and Procedures

One type of protection often overlooked is keeping backups. This could be because it often doesn't require getting new software, only a new mental outlook.

Several types of backup software are available. Your CD drive most likely came with backup software. If so, use it! If not, simply copying your important files to a memory stick or USB drive might be all the backup you need. For heavy users generating a lot of files or space-hogging photos, another option is to purchase an external hard drive. Today's hard drives are small in size, large in capacity, and cheap. For secure offsite storage, some people use an online storage site as well. We've actually done all of the above at our homes.

At a recent conference, we ran into a woman who spilled an entire bottle of water on her laptop in her hotel room. She was thousands of miles from home with a dead laptop and no way to get to the files she needed for her work. However, she had signed up for Carbonite's (www.carbonite.com) automatic backup service. She

bought a new laptop and was able to download all her files from the online backup the same day.

If you keep important records on your computer, say banking records or the college application essay you spent months on, you might want to keep at least one copy of your backup files at a place other than your home. That way if your house burns down or floats away, at least you won't lose your files as well. Incidentally, some people keep a home safe to store valuables and assume their backups will be safe in there as well. That's probably NOT the case. Remember the Ray Bradbury classic *Fahrenheit 451?* It's *paper* that burns at 451 degrees Fahrenheit. CDs, DVDs, and memory sticks will melt at much lower temps. Your beloved collection of banned books might be safe in a traditional home safe, but that extra copy of your computer backups is probably safest out of the house!

Don't forget! To be of use, backup files need to be fairly recent. How often that is depends on how often you use your computer and what you use it for. For most users though, once a week is the absolute minimum. So, select a time and a method and start backing up now!

15.5 Removal Tools

Defense doesn't always protect your system. Sometimes, you also need to clean up the mess when your computer protection fails. While it's best—and easiest—to think first and keep malware off your computer, you also need to know what to do when that fails.

If you use the Internet often enough and long enough, you're bound to get hit with something you're not prepared for. Everyone does. One day, Eric from Fairfax, California, came home from school with the Vundo.B virus on his system. Pretty scary, isn't it? How'd it happen?

Eric got nabbed in the gap. Every time a new virus is released, there's a little gap between when the virus hits the Net, when it's identified, and when the antivirus companies have added protection against that virus. Remember our talks about virus signatures? Eric was one of many gamers hit by a variant of Vundo.B after it was released but before that variant's virus signature had been added to antivirus software.

If that happens, and your machine is actually infected by a virus, often the only way to get rid of it is to run a removal tool. If that's confusing, keep in mind that the point of your antivirus software is to PREVENT you from getting hit with viruses and to identify any viruses you may have been infected with. The antivirus software isn't designed to get rid of each and every possible infection. That wouldn't be practical. Remember, there are over 100,000 pieces of malware out there with new code and new variants being released daily.

Once Eric's machine was hit with Vundo, it slowed down to a dead crawl. So slow in fact, that even Eric—a die-hard gamer and persistent blogger—finally gave up and quit using the machine.

This is what we did to learn about this virus and to get it off Eric's system. First, we went to the website for our virus protection software. Eric was running Norton Internet Security, so we went to the Symantec.com site and looked for information about Vundo.B. The description came up right away. It turns out that Vundo isn't actually a virus. It's a Trojan designed to drop adware onto the computer. It was easy to see why it was sucking up all of the resources from Eric's system. Next, we clicked on the link provided to download the removal tool. Eric's machine was too slow to even use at that point, so we downloaded the removal tool to another computer and copied it to a CD. Then, we took the CD to Eric's machine, copied the removal tool to his hard drive, and executed it. To all appearances, his machine was back to normal. Just to be safe though, Eric ran a virus scan and we made sure his antivirus software was up to date.

So long as you're running a full-service antivirus package, this procedure should work regardless of which company provides your antivirus protection.

15.6 Security Software Vendors

To select the best security solutions for your needs, you'll want to investigate and compare the products of at least several companies. As you do, you'll find that each company offers at least four or five (and sometimes more) packages providing different types and levels of protection. Since new products are released continually, we haven't listed individual products. We have, however, compiled a list of the top security software companies with general information about the types of protective

software provided by each vendor. For more information about specific products, visit the vendor websites. Also keep in mind that your Internet service provider may actually provide free security software. Comcast customers can download a free version of Symantec's security suite. Also, Microsoft's Security Essentials provides free antivirus software for their customers.

Company name & website	Anti-SPAM	Anti-Virus	Free Anti-Virus	Firewall	Free Firewall	Privacy Identity Protection	Parental Control/ Web Filters	Backup Software	Wi-Fi, Phone, or PDA Protection
AVG Security www.avg.com For free versions of products: www.freeavg.com	✔	✔	✔	✔	✔	✔	✔		
Avira www.avira.com	✔	✔		✔			✔		✔
CA www.ca.com		✔		✔		✔	✔	✔	
Carbonite www.carbonite.com								✔	
Comodo www.comodo.com	✔	✔	✔	✔	✔			✔	✔
Emsisoft www.emsisoft.com		✔		✔			✔		
ESET www.eset.com		✔		✔					✔
F-Secure www.f-secure.com	✔	✔		✔			✔	✔	✔
Immunet www.immunet.com			✔						
Kaspersky Lab www.kaspersky.com	✔	✔		✔		✔	✔		✔
McAfee www.mcafee.com	✔	✔	✔	✔	✔		✔	✔	
Microsoft www.microsoft.com	✔	✔	✔	✔	✔	✔	✔	✔	
Norman www.norman.com	✔	✔		✔	✔	✔			
Panda Security www.pandasecurity.com	✔	✔	✔	✔			✔		✔
Prevx www.prevx.com		✔							

continues

Security Software Vendors *continued*

Company name & website	Anti-SPAM	Anti-Virus	Free Anti-Virus	Firewall	Free Firewall	Privacy Identity Protection	Parental Control/ Web Filters	Backup Software	Wi-Fi, Phone, or PDA Protection
Sophos www.sophos.com	✔	✔		✔					
Sunbelt Software www.sunbeltsoftware.com	✔	✔		✔			✔		
Symantec www.symantec.com	✔	✔	✔	✔	✔	✔	✔	✔	
Trend Micro www.trendmicro.com	✔	✔		✔			✔		✔
Webroot www.webroot.com		✔		✔				✔	
Zone Labs www.zonelabs.com	✔	✔		✔	✔	✔	✔	✔	✔

Security Software Vendors

15.7 Keeping Your Security Software Current

Regardless of which software you select to protect your machine from malicious code, it is absolutely essential that you keep that software up to date. This means two things: configuring automatic updates and purchasing or downloading new versions of your protective software.

15.7.1 Configure Automatic Updates

When you set up your protective software, you'll have an option to select automatic updates. Do so! Each time you log onto the Internet (or at a specific interval, generally less than a week), your protection package will go off to its website and

Know Your Vendor!

Choosing the right protection against adware is essential. Choosing the wrong software can leave your system open to attack. In some cases, choosing the wrong software can even initiate an attack. Several makers of free "adware" protection are really Trojans that actually *install* adware on your system.

check for any important changes. Let's say that a nasty new virus has been released and is wreaking havoc on the Net. Your automatic update should automatically download and install the new signature to protect you from that virus, even if you haven't tuned into CNN and aren't aware of how much danger your data is in.

15.7.2 Buy the New Version

The methods used to attack computer systems change without notice. For every security hole patched, it seems a different black hat is designing a new and different delivery method. Don't kill an $800 laptop by skipping an update.

15.8 Keeping Your Security Awareness Current

Malware, attack forms, and computer security are often described as a moving target. That's not likely to change. That's why many large security vendors provide free security information on their websites. To keep yourself up-to-date, or to learn more about specific areas of computer security, you can also refer to the following resources:

Sites aimed at teens, schools, and families

- Common Sense Media (commonsensemedia.org)
- Cyber Smart (www.cybersmart.org)
- Family Online Safety Institute (www.fosi.org)
- FTC (www.ftc.org)
- Get Net Wise (www.getnetwise.org)
- iKeepSafe (www.ikeepsafe.org)
- i-SAFE (www.isafe.org)
- Look Both Ways (www.lookbothways.org)
- Microsoft Online Safety (www.Microsoft.com/protect)
- NetFamilyNews (www.netfamily news.org)
- Netsmartz (www.netsmartz.org)
- Web Wise Kids (www.webwisekids.org)

More general sites (for experts and would-be experts)

- CERIAS (www.cerias.purdue.edu)
- On Guard Online (www.onguardonline.gov)
- SANS Institute (www.sans.org)
- School Climate at the Center for Social and Emotional Education (www.schoolclimate.org)
- Searchsecurity.com (www.searchsecurity.com)
- Security Focus (www.securityfocus.com)
- Stay Safe Online (www.staysafeonline.org)
- Stop Badware (www.stopbadware.org)
- Wired Safety (www.wiredsafety.org)

Chapter 16

Tweaks

Alison spends a lot of time these days complaining about being the poor country cousin. Unlike her wealthy cousin Wesley, Alison doesn't have a top-of-the-line security bundle protecting her laptop.

Over the last six months, Alison's computer has been hit by three viruses, a Trojan, and at least five different types of adware. Wesley's computer has been fine. So while Wes is surfing the Net and playing games, Alison is lurking at spyware removal forums and on-hold with her Internet service provider. Alison complains frequently that Wes gets all the breaks.

Maybe. But money isn't everything when it comes to security. Alison could have avoided *all* the malware that's landed on her machine without spending a cent. The adware? That wouldn't be there if Alison didn't click first and think second. The viruses and Trojan? She could have avoided those as well, simply by applying patches and automatic updates.

In the last chapter, you learned about some of the protective products you'll need to keep your data safe. In this final chapter, you'll learn how to "tweak" the settings of software you already have in order to make your machine more secure. Those tweaks include the following:

- Setting the firewall first
- Patching security holes
- Using automatic updates
- Creating user accounts
- Password protecting all accounts
- Creating a password reset disk
- Testing the security you've set

16.1 Setting the Firewall First

At this point, it seems like we've said it over and over again… You open the box. You take out your brand new computer. You connect to the Internet? NO! If you do this, it's just a matter of time before your data is stolen or destroyed, or your system is used to attack other systems.

Before you start traversing that information superhighway, you MUST download any and all patches that you need to close up the security holes on your new computer. And, *before* you can do that, you need to have a firewall installed on your computer.

This may be confusing. In the last chapter, we talked about a firewall as a product that you can buy or a part of a bundled computer security solution. That's true. There are also several security programs including a firewall that you can download for free. Truthfully, there are a number of good firewall programs, free and commercial, and those firewalls include various features and functions that may make one a better choice for you than another.

On top of all this, your operating system will actually come with a firewall. How good that firewall is, and whether you will want to use that firewall or a different

one, will depend on which version of which operating system you're using. Windows 7, for example, comes with a good firewall.

If you decide to download a DIFFERENT firewall to use long-term, you still need to turn on your operating system firewall before you go to the Internet to download the new firewall. Think of your new computer as a car. Even if you plan to switch insurance companies next week, if you're driving your brand new car home from the dealership today, you want to tell your "old" insurance company. Otherwise, you could total your new car without coverage while you're driving to the insurance agent's office. Likewise, you don't want to total your new computer with malware while you're surfing to the firewall download site. That operating system firewall gives you at least temporary coverage while you're selecting and installing a long-term solution.

In some cases, you might want to use the operating system firewall as your long-term solution. That often depends on which security software you choose to use. Sometimes, that choice is made for you by your Internet service provider (ISP). Verizon, for example, provides McAfee security software free to their high-speed (DSL) customers. Comcast provides Symantec software free to their cable Internet customers. If you use either McAfee or Symantec security software, your operating system firewall will be turned off automatically during the installation of your security software. If you use an ISP that doesn't provide free security software, you may choose to download free antivirus software that doesn't include a bundled firewall. The free version of AVG, for example, doesn't include a firewall so Windows 7 users will want to continue to use the Windows 7 firewall.

Regardless of which operating system, ISP, or security software you choose, installing the firewall before downloading patches is crucial. Otherwise, an attacker can make his way into your computer before you have a chance to download the updates and close the holes.

16.2 Patching Security Holes

Much of the malicious code that protective software wards off can be avoided by making sure that any security holes in your operating system, application programs, and protective tools are patched as soon as those security holes are

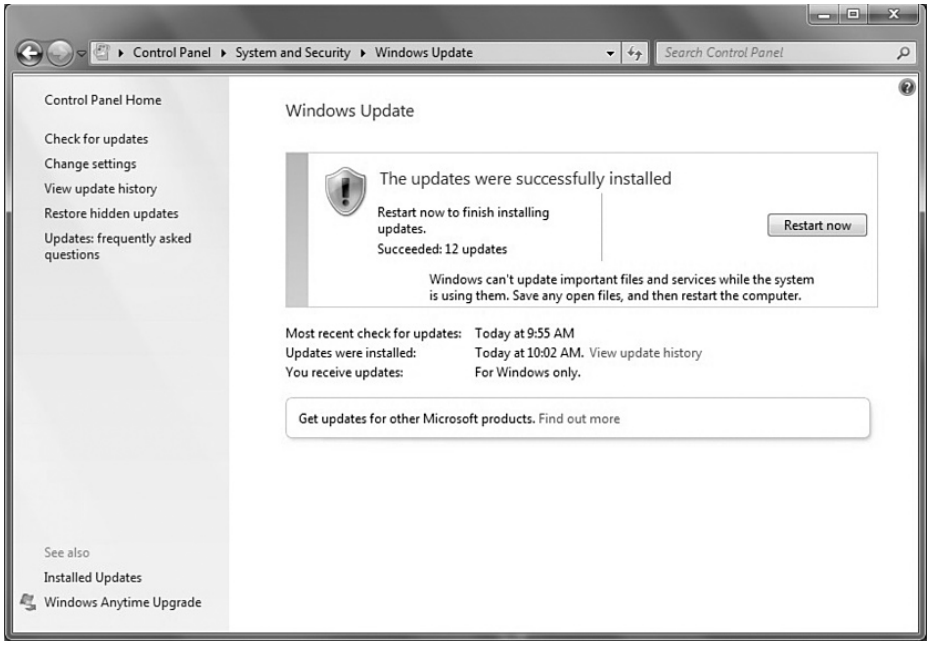
identified. Failing to do so can keep all those products we discussed in Chapter 15 from working properly, or in some cases, even working at all.

Once your firewall is on, you can select which antivirus software to run and then download patches right away. This is a step that far too many users forget. They assume that because they're setting up a new computer, nothing really needs to be updated yet. That's rarely true. Every day your new computer sat on the shelf at Best Buy or Staples, new malware and new variants on old malware were being released. Hackers and con artists were busy looking for new flaws to exploit and new ways to exploit old flaws.

If you use Windows, it's fairly simple to install any updates:

1. Click **Start**.
2. Choose **Control Panel > System and Security > Windows Update**.

   Once the updates download, you'll need to restart your computer to finish installing them.



New security flaws are identified every day, so staying updated with the current patches is critical. While you can do this manually (just repeat the steps above), the most practical approach is to use automatic updates.

16.2.1 Who's Looking for Holes?

Apparently, more people than you think.

Obviously, companies that make software are looking for holes in their own code to prevent problems they'll have to fix for their customers. At least let's hope they are.

Hackers are looking for holes because that's just what hackers do. Some hackers look for holes because they're interested in destroying, selling, or stealing corporate data. Some have a serious vendetta against a specific company and want to use security holes to embarrass or damage that company. Still others seek to profit by stealing personal information such as bank accounts and passwords.

There are almost as many reasons to look for security holes as there are methods to exploit them. There are also security experts whose business it is to look for holes. That is, they search for security vulnerabilities. Three of these companies are eEye.com, Secunia.com, and ISS.com X-Force (acquired by IBM). These companies sell protective software and provide information and **webinars** on the latest vulnerabilities. A webinar is an informational seminar that's held on the Internet. Webinar participants (students) all go to the same website at a specified time for a lecture or demonstration. During the webinar, participants can ask questions and interact with the "teacher." It's like a mini-class held online. Webinars are very popular with businesses because it's like sending employees to a conference for special training without having to actually send them and pay for airline tickets, hotel accommodations, etc.

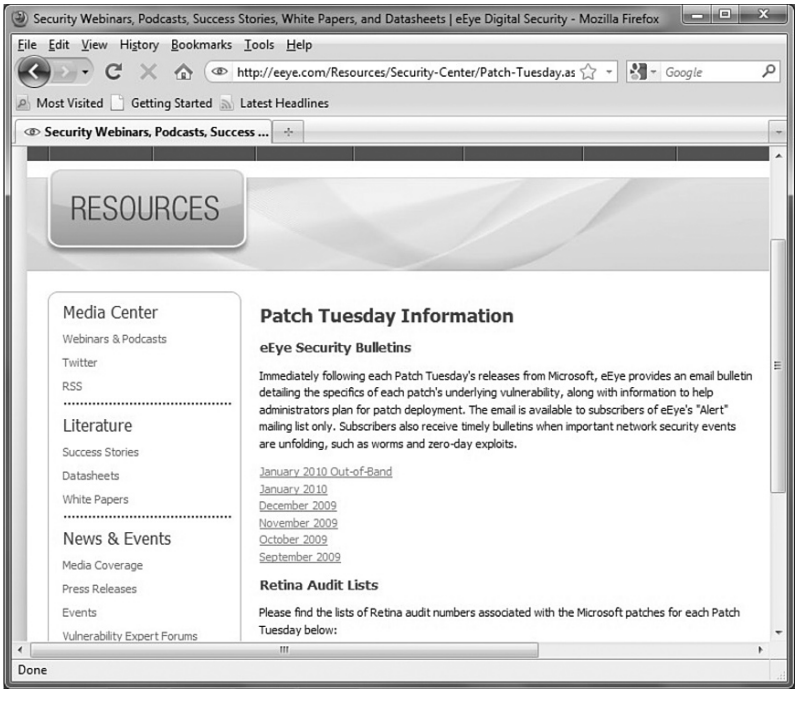
Webinar An informational seminar that's held on the Internet.

In theory, having professionals out hole-hunting seems like a really good idea. In practice, it doesn't always work out that way. Sometimes researchers who find holes report them to the public BEFORE the vendor has time to create a patch or to make that patch available for users. Of course, when we say vendor, we mean

the company that makes the software that includes the security vulnerability. In other cases, the vendor and the public—which includes the hacker community—find out about the flaw at the same time. Hackers then immediately begin releasing attack tools that exploit the new vulnerability.

16.2.2 Why Is Tuesday a Good Day to Update?

If you're going to run manual updates, the best day to do so is the second Tuesday of every month. Why? Microsoft announces new updates on the second Tuesday of every month. If you're curious what's actually being fixed in this month's Tuesday Patch, you can read an overview from eEye on their website. Just look under **Resources, Security Center, Patch Tuesdays**.



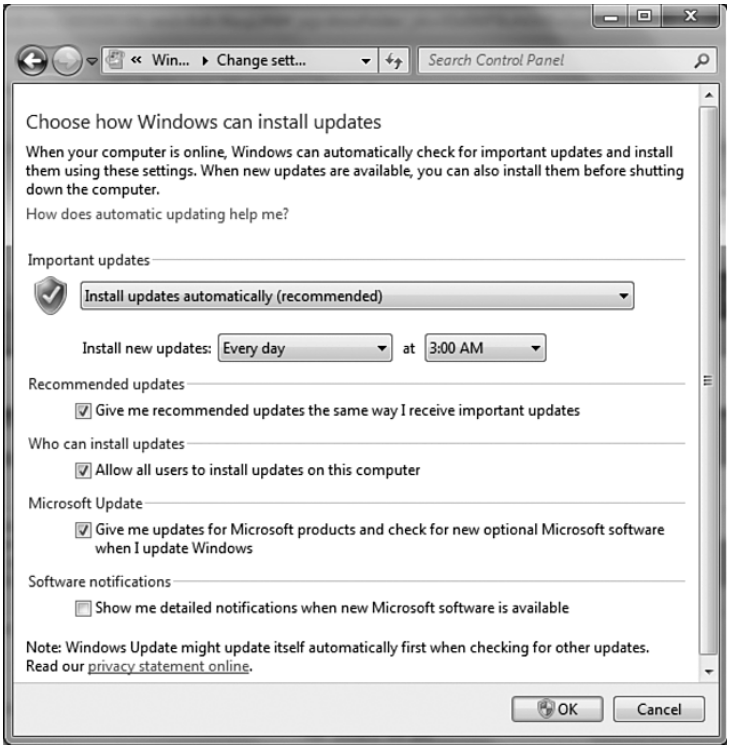
Are problems only ever discovered or fixed on Tuesday? Of course not. Microsoft announces *critical* patches outside of the monthly window. Since an update for a serious vulnerability can pop up any time, you really should update your computer every day.

16.3 Using Automatic Updates

The best way to make sure that security patches are fixed promptly on your computer is to use automatic updates. Because this might disrupt what you're doing on the computer, the best time to pick is a time you're not usually using the system.

In Windows 7, you can schedule automatic updates as follows:

1. Click **Start**.
2. Choose **Control Panel > System and Security > Windows Update**.
3. Click on **Change Setting**.
4. Select **Every day** and pick a time that works for you. Many users select 3 am since they're not likely to be using the computer at that time.



First Timer?

When you set up automatic updates for a brand new computer, it may take a while.

Why? The first time you run automatic updates, your computer will download all the security patches that were released since your operating system was installed. After that, it only needs to apply the "new" updates.

What happens if your computer isn't turned on at 3 am? Or if it's turned on but you're not connected to the Internet? No problem. Windows Update will simply run the automatic update the next time it can get to the Internet.

16.4 Creating User Accounts

Another way to protect your computer at no cost is to only use the Administrator account when you need to have administrative privileges. If you're not sure who the Administrator is—and you've never seen Admin as an option when you restart your computer—chances are very good that *you* are the administrator. If you don't know what that means, you need to.

16.4.1 What is an Administrator Account?

Windows 7 has four types of user accounts:

- A built-in Administrator account
- User accounts with administrator privileges
- Standard user accounts
- A guest account

Certain tasks can only be performed by **administrators**. For example, if your account doesn't have administrator privileges, you can't install new software.

Administrator The person in charge of maintaining a computer system. Administrators have special privileges not given to standard users.

Each type of user account has different privileges. A privilege is a type of permission. Your account privileges determine what you have permission to do. For example, there are three basic file permissions: read, write, and execute. "Read" means that you are allowed to look at a file. "Write" means that you can save

a file. This also means that you can change it. If you have "Write" permission, you can change a file that you've read and then save the changed copy. Finally, "Execute" means that you can run the file. (This assumes that the file is a program file. This is also why program files are often called *executables*.)

Since your account privileges determine which permissions you have, it makes a great deal of difference whether you are using a standard user account or a user account with administrator privileges. A common mistake that many people make is that they use one account with administrator privileges. Then, everyone in the house shares the same account. This can be dangerous.

There are a number of distinctions between the four types of user accounts.

Built-in Administrator Account

You won't see this account on the login screen because it's hidden from ordinary users. The only way to access this account is to restart your computer in Safe Mode. Why so secretive? Danger! The built-in administrator account has no restrictions. Using this account, you can make changes that could kill your computer if you don't know what you're doing. Unless you're a serious power user, we suggest you stay away from this particular account.

Administrative User Account

This type of account is for a regular user who has administrative privileges. Most home computers have one user account that has administrator privileges. The person with this account will be able to install and remove software and perform other administrative functions.

Standard User Accounts

Any number of people using your home computer might have a standard user account. Standard users are allowed to USE but not to administer. So, a standard user could create slideshows in Powerpoint, but he wouldn't be allowed to delete PowerPoint templates or uninstall Microsoft Office. An administrator, or a user with administrative privileges, would have the power to do all of those things. That's one reason you should be very careful about who gets administrator privileges. The more power a user has, the more potential he has to damage your system, even by accident.

Guest Account

The Guest account is just what it sounds like. This account is for someone who does not typically use the system. A guest user can access the Internet to check email and browse the web. However, a guest can't install software or hardware, set passwords, or change any system settings.

16.4.2 Why Are Standard User Accounts Good?

The more privileges your account has, the more things you have permission to do. This also means that any programs that run under your account also have more permissions. When you don't need administrative privileges, you should be using a standard user account instead. This does have a few minor drawbacks. Any time that you need to install software, you'll probably need to log off and then log back on using an administrative user account. However, this is a pretty minor inconvenience when weighed against the possibility of having your entire system destroyed.

16.4.3 How Do I Create a New User Account?

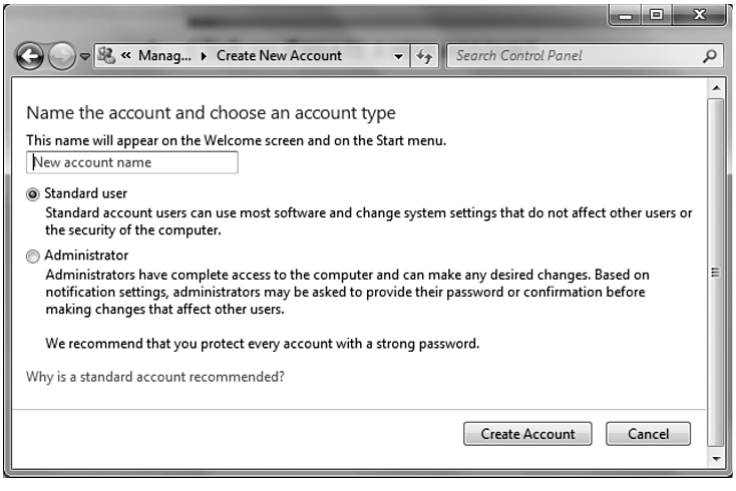
To create a new user account in Windows 7, do the following:

1. Click **Start**.
2. Choose **Control Panel > User Accounts and Family Safety > User Accounts**.
3. Click on **Add or Remove User Accounts**.

Ready to Take Charge?

Teens often make better system administrators than their parents simply because of the amount of time they spend using computers. The downside? Teens also use IM a lot more than their parents. Chatting with IM using an administrator account is risky. So is reading email, browsing the web, and downloading. If you're planning to make yourself the administrator, be sure to create yourself a standard user account as well. It's really safest if you don't spend ALL your time as Admin! If you want to learn more about administrator accounts, we recommend reading the book *Windows 7 Tweaks* by Steve Sinchak and browsing his website, tweaks.com.

4. Click on **Create a new account.**



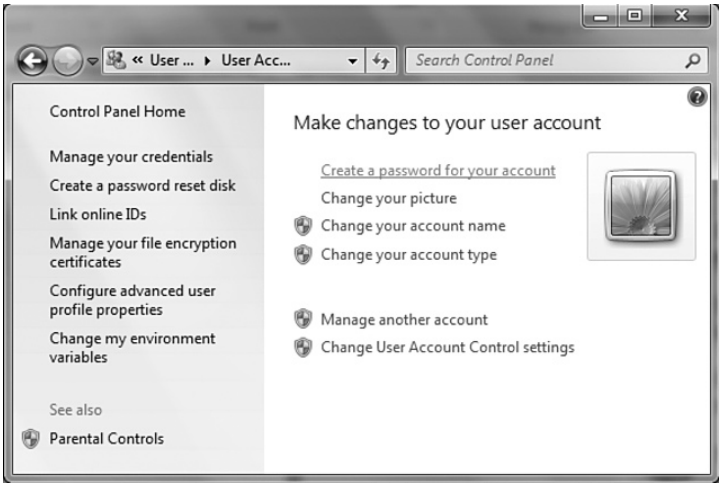
16.5 Password Protecting Your Accounts

At this point, you've set up two accounts for yourself: a standard user account and an administrative user account. You may also have set up additional user accounts for other people in your home likely to use your computer. Now what?

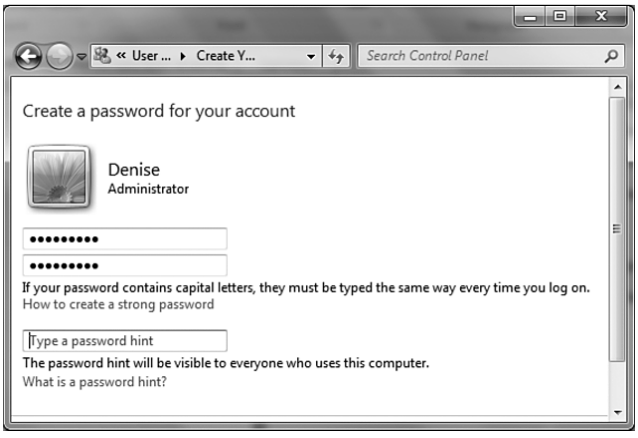
The last step in creating a new account is to properly password protect it:

1. Click **Start**.
2. Choose **Control Panel > User Accounts and Family Safety > User Accounts**.

3. Click on **Change your Windows password**.



4. Click on **Create a password for your account.**

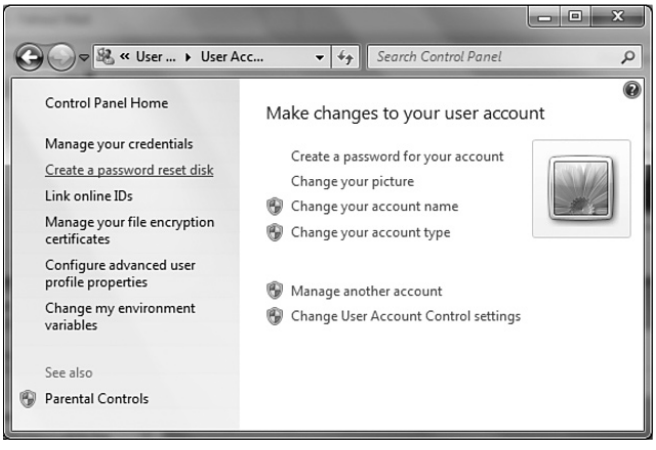


16.6 Creating a Password Reset Disk

The downside to password protecting your accounts is the danger of forgetting those password(s). You can protect yourself from that eventuality by creating a password resest disk or using a memory stick to store the password recovery file.

To create a password reset disk, do the following:

1. Click **Start.**
2. Choose **Control Panel > User Accounts and Family Safety > User Accounts.**
3. Click on **Create a password reset disk.**



4. Follow the instructions in the **Forgotten Password Wizard**.

While it sounds like this Wizard might help you if you've already forgotten the password, that's actually misleading. You need to create the **Password reset disk** BEFORE you forget your password!

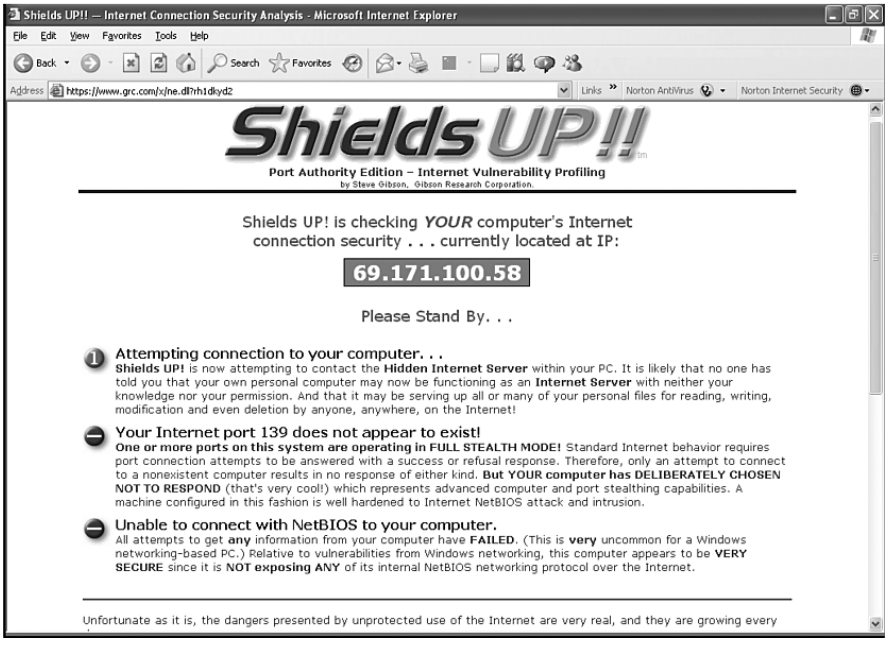
16.7 Testing Your Security

Once you install all of your security software, including your firewall, you need to test your security just to make sure.

Diamonds might be forever, but security is pretty ephemeral. You might install the world's most inclusive security setup today then have a new security flaw open up your entire computer tomorrow. That's why you can't just set it and forget it. The expert's mantra? "Configure security, test security, update security, keep your ear to the ground… Configure security, test security…"

OK, so it's not that catchy. But it is effective. And while it may not be 100% bullet proof, you'll at least have done everything humanly possible to ensure the safety of your data—for now. After all, no system is bullet proof. Or eternal.

Several vendors offer free security tests you can run over the Internet. These vendors include the big boys in security protection: Symantec, Computer Associates, and McAfee. Our favorite site, however, isn't one of the major security companies. We recommend Shields UP, a free site maintained by Steve Gibson at www.grc.com.



Of course, testing is only step one. If this test discovers a problem, you need to know what to do next. Imagine that your test results indicate a risky open port. Now what? You need to find out why that port is open, what the danger is, and how to close the port if you need to. We simply don't have enough space to go into every service and port, but open ports and risky services can open the door to bad guys.

Thankfully, this free site provides a detailed security list, descriptions of the risks, and recommendations on what to do if a test fails. They won't hold your hand, but they will provide you with enough details on any failed test to get you started in the right direction to fix the problem.

Appendix A

A Note to Parents

Congratulations! By allowing Internet access from home, school, or your local library, you've given your teen an onramp to the information superhighway!

With a few simple keystrokes, your teen now has access to encyclopedic knowledge, easy research on colleges and universities, and fast, reliable global communications. If you're like us and grew up just ahead of the digital generation, you're probably also still in awe of just how much the Internet really provides. Hopefully, you've not also been caught up in the backlash—distorted media coverage that seems to ignore the multitude of cyber-achievements and focuses almost entirely on the dark corners of cyberspace.

If your Internet savvy were based entirely on television news, you might think the web was filled with nothing but phishers, con artists, and potential molesters. Somehow, the billions of upright, honest netizens don't rate the evening news. Still, the dangers do exist. And avoiding those dangers requires knowledge, protection, and reasonable precaution. After all, you had your teen vaccinated against devastating diseases even though the odds of contracting polio in the Western world in the twenty-first century are much more remote than the odds of being phished online. It was a sensible precaution.

It's important to think about the technology you hand to your kids. Did you give your 10-year-old and your 16-year-old each an iPhone? Did you realize they'd have 24x7 100% access to the Internet? Are you concerned about what they might see or do online? Did you buy your 16-year-old a $1,000 laptop without knowing that you needed to add a firewall, apply patches, or set the antivirus software to automatically update?

You wouldn't hand your 5-year-old a book and expect him to find his way to school alone on the first day of Kindergarten. Even teens need your guidance on their way to the World Wide Web. To protect your teen online, consider these sensible precautions:

- Do what you need to do to protect your equipment. That includes antivirus software, spyware protection, and a good firewall. It also includes applying patches and updates.
- Realize that social networking sites aren't going away. If you're concerned, sit down together and review your teen's page on MySpace, Facebook, or Bebo. Drill your teen and friends about not giving out full names, addresses, school names, or other personally identifiable information.
- Keep young kids' computers in a public place. That means an open space where you can see what's going on—not behind a closed bedroom door. Once they become teenagers with laptops and have access everywhere they go, hopefully they will have learned the important safety tips.
- Keep your family business in the family. If you have a wireless network, make sure you're not broadcasting your network to the neighborhood.
- Avoid webcams. Teens are too often drawn to use webcams to post photos they may deeply regret in later life. Remove that temptation! Beware of laptops including bundled webcams.
- Don't be afraid to be the grownup. If you're concerned about your teen visiting inappropriate sites, install software with parental controls to block those sites. Remember when you child-proofed your kitchen with safety latches and electric plug guards? Especially if your child is a young teen, it's OK to "kid-proof" the Internet a bit as well.

- Don't be afraid to play the cop either if you need to. If you suspect your teen is doing something wrong online, strongly consider purchasing monitoring software. If your teen is doing something inappropriate, it's much better to be caught by a concerned parent than a real law enforcement officer.
- If you can, keep important data on your own computer, not the one your kids use. Think of this as protecting your teen's allowance or college fund! Particularly if your teen downloads software, music, or other items, you should keep your financial details and banking information on your own computer—not the one your teen uses to play games and download software from the Internet.
- If you can't afford a second PC, consider buying software designed to protect your financial transactions and personal information. Make sure you install that software if you're banking online or using the family computer for other financial transactions such as online bill paying or shopping.
- Remember that applying patches to close security holes isn't a one-time "do it, forget it" thing. New security holes pop up continuously. Configure your systems to use automatic updates to keep new holes patched.
- Remind your teen to think about the future. What teens post today will still be hanging around the Net years from now when they're working on developing real careers. Stupid comments and photos today can translate into unemployment in years to come.
- Watch out for social engineering. Just because someone calls you on the phone and tells you he is from the FBI, it doesn't mean he really is! Verify it. Teach your teens not to give out any personal information over the phone, email, IM, and so on, that could identify their location or provide key personal information.
- Be aware of cyberbullying. Lately, we've seen FAR too many news stories about teens who've been bullied to the point of suicide. Teach your kids to report cyberbullying if they see it and never to engage in it themselves.

- ***Scan the photos in your kid's phone from time to time.*** Sexting among teens (sending nude or semi-nude photos via text message) is a growing problem. Many teens caught doing this have been charged with sex crimes and labeled sex offenders for life. Don't let your kids get caught in this nightmare and ruin their lives. Teach them not to send or forward any photos of their private parts, or their friends'.
- Keep it positive! With the right security software and sensible precautions, there's no need to be afraid of the Internet. Your teen should take advantage of the wonderful opportunities it provides, and you should too!
- Get educated. You are the first line of defense when it comes to the safety of your kids on the Internet. Some great sites for you to learn more about online safety are Commonsense Media (commonsensemedia.org), Cyber Smart (cybersmart.org), FTC (ftc.gov), Get Net Wise (getnetwise.org), iKeepSafe (ikeepsafe.org), i-Safe (isafe.org), Look Both Ways (lookbothways.org), Microsoft Online Safety (microsoft.com/protect), NetFamilyNews (netfamilynews.org), Netsmartz (netsmartz.org), On Guard Online (onguardonline.gov), Stay Safe Online (staysafeonline.org), Stop Cyberbullying (stopcyberbullying.org), Web Wise Kids (webwisekids.org), and Wired Safety (wiredsafety.org).

Acknowledgments

The editors express their heartfelt thanks to all of the people who contributed their expertise and visions to this updated edition of ***Own Your Space***. We'd like to offer special thanks to the teens and young adults in our lives—Eric, Douglas, Tabitha, Nina, Kayla, and Nathan. By so graciously downloading worms, accepting viruses, and unknowingly installing pernicious adware, they unwittingly introduced us to the dangers the Internet poses to unsuspecting families.

Thanks also to all of the security experts joining our team for the next version and to the experts who lent their skills and efforts to this version:

- Jack McCullough for updating the wireless section
- Richard Ford for his malware expertise
- Keith Watson for both content updates and his idea to produce a free online version of this book.

A special thanks to Eric (17) for leading our teen discussions and working with the web designers and cover artist. We want to ***especially*** thank all the teens who generated ideas, shared experiences, and provided feedback. This book would not exist without those teens. While we've omitted their last names to protect their privacy, we really can't overstate just how important their feedback was to this project.

Contributors

Jack McCullough
Wireless Security Expert
Security Consultant and Author

Keith Watson
Security Researcher

Linda McCarthy
Security Researcher

Richard Ford,
Harris Professor of Assured Information,
Florida Tech

Denise Weldon-Siviy
Writer, Editor, Teacher, and Mom

Eric (17) Novato, California
Teen Insight

Brian (17) Novato, California
Teen Insight

Hala (17) Pleasanton, California
Teen Contributor

Tabitha (17) Littlestown, Pennsylvania
Teen Contributor

Kayla (15) Gettysburg, Pennsylvania
Teen Contributor

Gino (13) Lodi, California
Teen Contributor

Dominic (11) Lodi, California
Teen Contributor

Waqas (14) Tacoma, Washington
Teen Contributor

Index

M

N

O

P – Q

T

U – V

W

X – Z

OWN YOUR SPACE

KEEP YOURSELF AND YOUR STUFF SAFE ONLINE

THE BOOK FOR TEENS THAT EVERY PARENT SHOULD READ!

A collaborative project to provide free security learning to teens and families online, made available under the Creative Commons Licensing, and made possible by the support of individual and corporate sponsors.

Every day, millions of American school children log on or log in and make decisions that can compromise their safety, security, and privacy. We've all heard the horror stories of stolen identities, cyber stalking, and perverts on the Internet. Kids need to know how to stay safe online and how to use the Internet in ways that won't jeopardize their privacy or damage their reputations for years to come.

Learn how to

- Kill viruses, worms, Trojans, and spyware
- Deal with cyberbullies
- Give SPAM the curb and smash web bugs
- Understand just how public your "private" blogs are
- Keep wireless freeloaders off your network
- Prevent sexting from ruining your life

About the team

Linda McCarthy, the former Senior Director of Internet Safety at Symantec, wrote the first edition of *Own Your Space*. With 20+ years experience in the industry, Linda has been hired to test security on corporate networks around the world. For the 2010 edition, Linda's expertise is backed up by a full team to provide the best security experience possible for teens and families online. That team includes security experts, design experts, anime artists, and parent reviewers, as well as a dedicated group of teen reviewers, web designers, and test readers.

General Computing

ISBN 978-0-615-37366-9

51999>

9 780615 373669

$19.99 US / $24.99 CAN

Cover design: Alan Clements
Cover artist: Nina Matsumoto

www.100pagepress.com

page press
Smart Books for Smart People®