# Table of Contents

**Introduction** ................................................................. 1  
About This Book ................................................................. 1  
Icons Used in This Book ....................................................... 2  
Where to Go from Here ......................................................... 2  

**Chapter 1: Safeguarding Your Identity** ......................... 3  
Assessing Your Information .................................................. 4  
Protecting Your Privacy ....................................................... 5  
Dealing with Privacy Thieves ............................................... 6  
  How thieves obtain your info ............................................. 6  
  What to look for in privacy policies .................................... 8  
Responding to Identity Theft or Fraud .................................... 9  
Knowing Your Resources .................................................... 10  

**Chapter 2: Protecting Yourself from Viruses, Spyware, and Scams** .................................................. 13  
Identifying Common Ways Information Is Compromised... 14  
  Viruses ........................................................................ 14  
  Worms ......................................................................... 15  
  Macro viruses ............................................................... 15  
  Trojan horses ............................................................... 16  
  Bots ........................................................................ 16  
  Spyware ....................................................................... 16  
  Rootkits ..................................................................... 16  
Protecting Yourself ............................................................. 17  
Recognizing Scams ............................................................... 18  
  Gone phishing ............................................................. 18  
  Looking for love ............................................................ 19  
Health care scams ............................................................ 19  
Bogus charities ................................................................. 20  
Bogus invoices ................................................................. 20  
Phony investments ............................................................ 21  
Temporary account suspension .......................................... 21  
Job scams .................................................................. 22
Chapter 3: Password Secrets ........................................ 23
Where Do I Use Passwords? ........................................ 23
Choosing and Protecting Passwords .......................... 24
Storing and Recalling Passwords .............................. 25
Understanding Password Vulnerabilities ...................... 27
Using Encryption................................................ 28
Appreciating Password Enhancements ......................... 29
Answering Security Questions...................................... 30

Chapter 4: Risk-Free E-Mail ............................................ 31
Following E-Mail Safety Basics .................................. 32
Creating Safe E-Mail Aliases ..................................... 33
Hiding Your Name in E-Mails .................................... 35
Opening an Attachment ............................................ 35
Managing Spam ..................................................... 36
Using Spam Filters ............................................... 36
Filing a Spam Complaint ......................................... 37
Recognizing Fraud and Scams ................................. 38
Avoiding the Latest E-Mail Scam of the Day .............. 39
Avoiding Phishing ................................................ 39

Chapter 5: Shopping and Banking Safely ......................... 41
Vetting Websites Critically ...................................... 41
Considering Online Versus Offline Banking ............... 42
Evaluating an Online Shop ....................................... 43
Guarding Your Card Online ...................................... 44
Ordering stuff without sharing your primary account information ....................................................... 44
Embracing safe shopping practices .......................... 45

Chapter 6: Ten Things You Can Do Today to Protect Yourself ................................................. 47
Use Two-Factor Authentication .................................. 47
Stay Safe While Gaming .......................................... 47
Secure Your Public and Private Wi-Fi Connections ....... 48
Understand and Use Privacy Settings on Social Media Sites ................................................................. 48
Protect Devices with Passwords ............................... 49
Choose Carefully Whom You Share Personal Info with Online ................................................................. 49
Give Up On Safe Ways to Back Up Your Files Online .... 49
Consider Location Settings on Devices ..................... 50
Create a Google Alert for Your Name ....................... 50
Surf Privately in Public .......................................... 51
Introduction

The Internet has become an integral part of our lives in the blink of an eye; it’s been only about 20 years or so since the web came on the consumer scene, and now many of us couldn’t imagine life without it. We use it to check news stories, watch movies, balance bank accounts, buy any number of products and services, share photos, and communicate with others.

But you — like many people — may worry about some of the risks the web harbors. This book can help you understand what’s going on out there, arm you with the skills to keep you safer, and show you how to enjoy your online time with greater peace of mind.

About This Book

This book is packed with information written specifically for anyone who uses the Internet and has an identity to protect — that would be you. Read it. Learn it. Pass it around to family members, coworkers, and friends, and make them read it. The more protected they are from being hacked, the more protected you are from dealing with someone who has been hacked, and perhaps exposing you.

Because Microsoft Windows-based PCs are the most common type of computers, this book focuses on Windows functionality. But rest assured that the majority of the advice in this book about staying safe online works no matter whether you use a Mac, a Windows-based PC, or a Linux machine. And because mobile use is quickly catching up with computers, we also include information about how to protect yourself when using mobile devices.
Icons Used in This Book

This book uses certain conventions to help you find your way around, including the following:

Tip icons point out insights or helpful suggestions.

Remember icons indicate important details that will serve you well in years to come if you remember them.

Warning icons indicate online behaviors that might put you, your information, your loved ones, or your pocketbook in jeopardy.

Where to Go from Here

Whether you use a computer every day or are just starting to use the Internet, working your way through this book could help you become even savvier than your grandchildren or the kid next door. You don’t have to read the chapters in order; this is a reference book, so if you’re concerned most about passwords, for example, go to Chapter 3. A good, solid place to start, as with any book, though, is Chapter 1.
Chapter 1

Safeguarding Your Identity

In This Chapter
▶ Identifying private information and where it is online
▶ Keeping your private information private
▶ Eliminating privacy pests
▶ Taking swift and effective action if your identity is stolen

It’s all too easy to share information about yourself online these days, whether you’re active in social media or shopping online. Overall, this book helps you guard your online activity, and this chapter specifically helps you understand the kind of information that you’re asked to provide online and the potential ramifications that can occur if that information falls into the wrong hands.

By using your personal information, identity thieves can “party hard” on your nickel and your good credit reputation. They spend like there’s no tomorrow because they know that someone else (you) is picking up the tab.

Identity thieves can use your personal information to open accounts, such as a cellphone account, in your name. Of course, they skip paying the bills and continue to use the phone until you discover the theft and take action; then they drop that account and move on to another unsuspecting victim. Worse, even major corporations that you trust can be compromised and leak your information whether you do anything wrong or not.
Assessing Your Information

To get started, take stock of the information you may have out there on the Internet and the risk it poses if it’s stolen. Sensitive information involves numbers and other key facts about you that together comprise your paper and online identities. The vulnerable personal information that identity thieves use is described in this list:

- **Social Security number (SSN):** Your 9-digit personal identification number (assigned by the federal government) is the key to the kingdom for identity thieves: The identity thief uses your SSN to apply for credit, file false tax returns, get a job, open bank accounts, and so on.

- **Date of birth (DOB):** A DOB is a piece of the personal information puzzle that really isn’t a problem if that’s all the information the bad guys have, but put together with other information, it lets an identity thief become you.

- **Security questions:** You see these questions — asking for your first pet’s name and where you attended high school, for example — when you’re setting up an online account.

- **Mother’s maiden name:** This name is used to verify your identity when accessing financial information.

  Security questions have begun to include a father’s middle name as well. Everybody gets equal time!

- **Personal identification numbers (PINs):** These are usually 4- (or more) digit numbers used to access your bank accounts online or when using your ATM card.

- **Passwords:** Your passwords — which are the keys to any information stored electronically — are discussed in detail in Chapter 3.

- **Driver’s license number:** A thief who has your driver’s license number can make a phony license that shows your name and driver’s license number with his picture.

- **Social media posts:** This information can convey where you live — or even where you are right this minute — your alma mater, your likes and dislikes, and other information that people can use to form a complete
picture of who you are. Think about all the information you’ve distributed on these networks (both new and old — hello, MySpace and Friendster!) and how likely it is that somebody could unearth this information by looking quickly on a search engine. Even if you deactivate or delete your account, that information can still be accessible via cached searches and archives.

Give only the minimum information necessary to any online source, and make sure you know who’s receiving the information.

**Protecting Your Privacy**

After assessing information but before posting that information on a social networking site such as Facebook, Google+, LinkedIn, Instagram, or Twitter, carefully review your privacy settings. Sharing publicly is the default, and you have to go out of your way to not do so.

When posting information that appears on a public website, such as when you leave comments on articles you read, offer reviews of restaurants or movies, or post in any discussion venue, don’t use your full name. This advice doesn’t apply if you’re working in a business context, such as posting information on your company’s website.

Never provide your name, address, phone number, Social Security number, or drivers license number to someone you don’t know.

Never believe anyone who says that he’s from Facebook tech support, eBay fraud prevention, PayPal administration, your bank, or a similar-sounding authority and asks you for your password. No legitimate entity will ever ask you for your password.

Be especially careful about disclosing information about kids. Don’t fill out profiles that ask for a kid’s name, hometown, school, age, address, or phone number, because they’re invariably used for “targeted marketing” (also known as junk mail).
Dealing with Privacy Thieves

So if you control who accesses your information, how is it that people still find a way to creep into your online life and ask you for more? Let’s take a look at the most common ways to access details about you on the Internet.

How thieves obtain your info

Here you are, sitting and reading this book about passwords. Can you begin to hear the faint scratches of the privacy pests as they claw away at the walls of your electronic security?

No? Then it’s time to start looking in some of the mustier corners of your daily activities to see whether you can spot any telltale signs. As an example, look at an everyday action, such as buying a book. The last time you bought a book online, did you buy it . . .

✔ Over the Internet? Did the website ask you for any personally identifiable information — your mailing address, perhaps, or an e-mail address? By downloading a book over the Internet, for example, you reveal certain information about yourself to the bookseller. As you continue to read this book, someone at the site may be adding that information to all the other personal data that has already been collected about you based on all the other items you’ve purchased — or even just looked at — while on that website.

✔ While browsing the web at home? If so, you may have revealed to your Internet service provider (ISP) some information about yourself, including your interests and purchasing habits. As you continue reading, someone may be adding that information to all the other personal data that’s already been collected about you based on all the places you’ve surfed and the things you’ve bought online.

✔ While browsing the web at work? If so, you may have revealed to your employer some information about yourself. Luckily, you weren’t looking for job-hunting books. Oops! You were looking for those, too? Whatever the case, someone may be adding that information to your personnel file now, along with all the other personal data that’s already been collected about you because your employer has the legal right to monitor you and record every move you make on the Internet while you’re at work.
✓ Using an insecure Internet browser? If you’re using an older Internet browser or if you have neglected to update your browser when newer versions are available, you may be making yourself more vulnerable. You may have revealed information about yourself to a hacker in a far-away place who may have already targeted you as the one whose credit card number will buy her a new video game system — or maybe even a wardrobe or new car. While you’re reading now, she may be busy collecting additional information and building an intimate profile of you that she can use to fraudulently spend your money, online and offline.

Follow these steps to help reduce your privacy concerns when buying online or performing other transactions with sensitive data:

✓ Don’t submit your personal information on computers you don’t own. This includes your work computer. If you don’t want people seeing what you’re typing or viewing on the Internet, restrict your activity to your own computer. Your boss will probably be happier that way, too.

✓ Set your web browser to private browsing. The gist of the private browsing function is that the browser doesn’t store cookies or track browser history while in this mode. You may forego some of the convenience of browsing the web, but you gain a measure of privacy. Different browsers name the feature differently: Chrome calls it Incognito Mode, Internet Explorer calls it In-Private Browsing, Firefox calls it Stealth Mode, and Safari calls it Private Browsing. All browsers have the feature accessible easily via their main menu (the Safari menu in that browser).

✓ Don’t give out personal information, including your e-mail address. Even if you’re trying to win a fabulous prize, be aware that the company running the contest wants your personal information to better track and market to you. Opt out of any mailings or consider the e-mails you get a trade-off for the service you sign up for, and maybe even use a dedicated e-mail account for the spam you’ll likely receive if the lure of the prize is too great.
What to look for in privacy policies

Have you ever seen the magicians Penn & Teller vow never to show you how their magic tricks are done — and then play the old shell game with a small ball hidden under one of three clear plastic cups so that you can see exactly how they perform the trick?

We are about to perform the privacy lawyer’s equivalent of that trick by showing you what you should look for in a privacy statement as though you were reading it through the clear plastic lenses of the sneakiest, most cynical lawyer in town. Ask yourself whether a website’s privacy policy tells you

✔ Explicitly what information the website is collecting: Is the site getting your name and address? Your e-mail address? The IP address of your computer? Your credit card number? The combination to your gym locker or to the hidden safe in the den? If the site doesn’t say exactly what information it’s collecting, you should assume the worst.

✔ How your information will be used: Here’s where the most advertising-speak usually happens, and you have to read carefully to figure out what the site is saying before deciding whether to register on the site. Will the company drive you crazy by sending you catalogs by snail mail and e-mailing you ads by the dozens? Will it sell your personal information to other advertisers? Is the benefit it offers in return — a promo code, coupon, or advance notice of sales, for example — worth any potential annoyance?

✔ Whether and how you can opt out of having the site collect information about you: Some sites offer you the option to opt out of the data collection. For example, you may have a choice to set up a personal account so you can return to the site without reentering your information, or to use a generic guest account which does not store your information. If you don’t want a company to collect information about you, and this option is not offered, you may want to visit the competition.

✔ How the site protects your information: Does the site use encryption to keep bad guys from snapping your personal information as it passes between your computer and its own? Does it have security measures in place to prevent people from stealing your information from its databases?
Sites are sometimes vague about specific security measures, and that’s a good thing. Providing too many specifics gives crooks an edge, and the unknown keeps them guessing. If the site’s policy fails to mention security or doesn’t assert that it’s using industry best practices, your privacy and security may not be protected.

✓ Who is responsible for making sure that the site lives up to its promises: Many e-commerce firms have appointed chief privacy officers and other dedicated personnel to manage their consumer information practices and to be the point person in ensuring that all promises made in a privacy policy are honored. If a site’s policy doesn’t say who has responsibility for overseeing the privacy of your data, you’re better off assuming that the answer is nobody.

You’ll also want to review the privacy policies of the apps you use on your smart device of choice. Make sure you look at the settings for all the apps you use and see how they want to use your information, weighing that against how much you want the app. Scrupulous developers ask you for your permission (usually in an alert where you must click Yes or No) to use your information or to gain access to contact information on your phone, but not all app developers may be so scrupulous. Check all settings in an app, and don’t be afraid to delete apps that don’t play by the rules. Plenty more apps are available to take their place, in many cases for free, although all free apps tend to have some cost (your e-mail address, for example) to give you the services you need. Again, it’s a trade-off.

Responding to Identity Theft or Fraud

If identity theft happens to you, act immediately! The following items are in no particular order because the order might well change depending on what’s happened to you.

✓ As soon as you identify which accounts have been compromised, contact those providers immediately.

✓ Contact the three major credit bureaus: Equifax, Experian, and TransUnion to secure your credit.

• You can find contact information for these organizations at www.consumer.ftc.gov/articles/0155-free-credit-reports.
• Tell each bureau that you’re the victim of identity theft, and report your ID as stolen. Because you’re the victim of identity theft, the three bureaus will each give you a copy of your credit report for free.

• Ask all three credit bureaus to flag your file with a fraud alert and add a victim’s statement to your file. The statement can be as simple as this: “Someone is using my ID to fraudulently apply for credit. Before new accounts can be opened, I must be contacted at <your phone number>.”

• Ask all three credit bureaus to tell you the names and phone numbers of all creditors with whom fraudulent accounts have been opened. Contact each of these creditors to report the identity theft.

• Ask each credit bureau to clear your file of all inquiries that have been generated as a result of the fraudulent use of your information.

• Be sure to request and check your credit reports every few months to watch for new incidents of fraud. You can do this free once a year through each of the three bureaus.

✓ Report the identity theft to your local law enforcement agency. Insist on filing a written report.

✓ Monitor all other financial records (incoming mail, phone bills, credit card bills, and bank statements, for example) for signs of other fraud.

For the most up-to-date information on how to protect yourself against identity theft or to see what to do if it happens to you, visit www.privacyrights.org and www.consumer.ftc.gov/features/feature-0014-identity-theft.

Knowing Your Resources

You aren’t alone in the fight against identity theft. From the federal government and credit card companies to your local police, your allies abound and can help you with many aspects of identity theft. Here are some of your key sources of help:

✓ The Federal Trade Commission (FTC): The FTC provides information that’s useful for preventing identity theft and knowing what to do if you’re a victim. Its
website ([www.consumer.gov/idtheft](www.consumer.gov/idtheft)) is chock-full of statistics, information, forms, and more to help you understand and prevent identity theft as well as what to do if you’re a victim. **When you file a complaint online, the report is forwarded to law enforcement as well.**

- **Most local law enforcement agencies:** These agencies provide information on how to prevent identity theft and what to do if you become a victim. Examples include the county sheriff’s office, local police, and so forth.

- **Federal law enforcement agencies:** The most active federal law-enforcement agencies investigating ID theft are the U.S. Postal Inspection Service and the U.S. Secret Service. You won’t contact these agencies directly, but if you contact the proper authorities for a given crime, such as postal fraud, at least one of these agencies will likely join in on the investigation.

- **Internet Crime Complaint Center (IC3):** The IC3 ([www.ic3.gov](www.ic3.gov)) is a partnership between the FBI and the National White Collar Crime Center (NW3C). At the website, you can file a complaint and read about recent scams and other news. The IC3 reports the complaints to whichever local authorities are in charge of handling the situation.

- **Federal Bureau of Investigation (FBI):** Go to [www.fbi.gov/scams-safety](www.fbi.gov/scams-safety) to find more information. Check out their site for a great deal of useful information, including their Scam Alert feature.

- **The Social Security Administration (SSA):** The SSA has guidelines for reporting fraud on its website ([www.ssa.gov](www.ssa.gov)). Also, you need to submit a fraud-reporting form to the SSA Office of Inspector General (OIG), an investigative branch. The SSA recommends downloading the form, completing it, and then sending it via fax or regular mail to ensure confidentiality. When you report the use of your SSN for identity theft, the SSA doesn’t investigate the identity theft but looks into benefit fraud instead.

- **Financial institutions and credit card companies:** Most financial institutions provide tips about preventing fraud and knowing what to do if you’re a victim. Some institutions provide discounts and links to sites that charge an annual membership fee for providing identity theft protection. For example, I subscribe to a CreditExpert.com service, and the site is part of the credit bureau Experian.
To help stem the upward trend of credit card fraud, the card-issuing companies monitor and look for irregular patterns of use. The credit card companies monitor what you charge per month, and when a purchase varies from your typical pattern, the card company calls and asks whether you made the purchase. For example, when people go on vacation and don’t notify the card company, they’ll probably receive a call asking whether they made a purchase in X country or Y state. The card companies have used this method for many years, and it’s helped reduce some credit card fraud.

* AARP Fraud Watch Network: AARP’s Fraud Watch Network links you with experts, law enforcement, and people like you who are on the lookout for scams. It offers the latest alerts from state Attorneys General and other local officials. Visit www.aarp.org and type “fraud watch” in the search box.

* Experienced attorneys: Although the resources we list here are usually quite helpful, you may want to contact an attorney to help you restore your credit and name if creditors aren’t cooperative in removing fraudulent accounts from your credit report or charges from accounts. Contact the American Bar Association or the Legal Aid office in your area and ask for the names of attorneys that specialize in the Fair Credit Reporting Act (FCRA), consumer law, and the Fair Credit Billing Act.

* Your state’s Attorney General’s Office: Check the website for your state’s attorney general’s office, which has resources about identity theft prevention.
Chapter 2
Protecting Yourself from Viruses, Spyware, and Scams

In This Chapter
▶ Uninviting hackers to your Internet party
▶ Protecting yourself from viruses
▶ Identifying scams

It doesn’t matter how you do it; from the minute you connect your computer to the Internet, you’ve hung a giant neon Welcome sign in front of your humble little cyber-abode.

Software companies have improved their security policies over the years, but they’re still not perfect. Programs and operating systems still ship with security flaws. Why? Because security features cause operating systems to become complicated, and in the battle between high security and user friendliness, guess which one usually wins? Unfortunately, many of the holes are extremely difficult — if not impossible — for most users to find and turn off. On top of that, lots of popular Internet programs find their way into your device’s information. It doesn’t matter if it’s a home computer or a mobile device — everything has some kind of security hole in it.

Some of the scariest horror movies begin at home. Bad situations just seem a little more horrifying when they happen close to you. This chapter looks at some of the more common troubles you can encounter online and what you can do to avoid these terrors.
Identifying Common Ways Information Is Compromised

As you read about viruses and other threats to your computer, you might be astonished at just how many kinds of malicious activities are lurking online. Keep in mind, however, the more you know about the threats, the better you can protect yourself from online mischief.

Viruses

A virus is a type of little program that loads onto your computer without your knowing it and then starts running amok. Viruses are so named because they act just like biological viruses in the way they replicate themselves through networks, just like a biological virus replicates itself in the body. This section describes a few of the defining characteristics of a virus.

A virus can replicate itself and pass itself along to infect other computers — but only by burying itself inside a larger vessel, such as a Microsoft Word document or the programming code of a piece of software, which then takes a ride to another computer on a thumb drive, disk, or as an e-mail attachment or by some other method of file transfer.

In replicating themselves, viruses sometimes do their damage by making so many copies of themselves that they fill up your computer’s memory and cause it to crash.

In many cases, the replication and spread of a virus are secondary to its primary function, which is to perform some other task (sometimes harmless, sometimes electronically fatal) inside your computer. For example, a more malicious virus may take complete control of your computer and order it to do something horrible, such as delete its own hard drive. Other viruses are intended as mere pranks: A good example is the Merry Christmas virus that simply flashes a harmless season’s greeting on your screen in December — end of story, or so you think. But now it’s April Fools’ Day and the Merry Christmas virus doesn’t let you boot up your computer. Ho-ho-ho!
Worms

Forgive the analogy, but think tapeworms — the ones your mom always thought you had in your gut when you were a kid eating everything in sight. Here’s why the analogy is so fitting. Worms are similar to viruses in that they can copy themselves and do bad things to the computers they invade. Worms are also notorious loners, though, so they generally don’t attach themselves to the programming code of files or dig deeply in the out-of-the-way corners of disks, thumb drives, or hard drives, as viruses do. Instead, worms send copies of themselves over the Internet directly, or they can hitch a ride in an e-mail message. Melissa and MyDoom are the names of two of the nastier worms to be hatched in recent decades.

Macro viruses

A macro virus is a unique type of virus: It makes its appearance in the form of a macro embedded in a document file, rather than as a program or application.

Some experts claim that nearly three-quarters of all viruses are macro viruses, in part because they can embed themselves in your software and attach themselves to every document you create, which allows them to spread easily to others.

To understand macro viruses, you first have to understand macros. Many software applications, including Word, Excel, and PowerPoint, allow you to create macros, which are nothing more than a way to record long series of commands and then repeat the series of commands over and over again with just a keystroke or two.

In some cases, macro viruses add themselves to your default document template. Every time you create a new document in Word, the document is based on a default template named Normal.dotm that can contain font choices, margin settings, and, yes, even macros and macro viruses. If a macro virus is in your default template, you spread the virus every time you open or create a new document. That’s how most macro viruses spread so quickly.
Trojan horses

A Trojan horse program tricks you into loading and running it by pretending to be something that it’s not. (You might remember this story from Greek mythology.) The perfect example of a Trojan horse is a file that masquerades as an antivirus software patch but is really malware. If a Trojan horse has taken hold of your computer, you will notice your PC behaving strangely, most notably with Web browsers redirecting you to pages you didn’t intend to visit. Some Trojan horses are coupled with other types of viruses, such as macro viruses, which then generate new Trojan horses that are passed along to others.

Bots

After a malicious entity infects a computer, it can gather computers together to perform specific tasks, such as spam several million e-mail accounts or try to take down a server. An infected computer is a bot, and many bots gather to form botnets. It’s not bad enough that your computer is infected, it also becomes a zombie PC, which essentially is at the behest of the hacker and does his bidding whether you know it or not. Botnets are armies of zombie PCs gathered to perform hideous tasks (and probably gather more victims like themselves).

Spyware

Computer privacy experts define spyware as any piece of software that gathers information and uses your Internet connection to send that information somewhere else on your computer without your knowledge or approval. But why does the spyware do this? In many cases, the spyware is gathering information about you and your activities on your computer and sending that data back to the software manufacturer or another data-collection company so that it can know more about you. Keyloggers, which record your keypresses on your keyboard and send them to data thieves, are a prime spyware tool.

Rootkits

Rootkits are the most insidious type of malware, with the ability to hide as legitimate system processes to fool antivirus software. They also are able to attach themselves to the
BIOS software responsible for starting up a computer before the operating system engages, allowing the malware to even survive a reinstallation of your operating system.

The antivirus software programs described in the following section can help protect you from rootkit and other types of attacks.

**Protecting Yourself**

Because you can’t spend your life installing updates, here are some rules of thumb to figure out what updates you really need.

Install antivirus software (like Norton or McAfee, or use a free version, like AVG, Avira, or BitDefender). Newer operating systems, such as Windows 8, can even have virus protection built in. And then remember to update your antivirus software consistently. Having the software is good, but without updated antivirus definitions that fight against current viruses — which are written and released almost every day — your antivirus software doesn’t do you much good. Antivirus software manufacturers are continually updating these definitions, and you must get their updates from the web at least once a month — and every time you hear about a new virus that’s storming the computer world like a plague.

More recent antivirus software packages automatically update their own definitions from the Internet so that you don’t have to. If you’re forgetful at times, you should invest in one of these auto-updating antivirus software programs, even if an antivirus program is already installed on your computer.

The best way to make sure that your computer hasn’t been hijacked is to run antivirus scans regularly. If your computer is connected to the Internet 24/7, you should also run a personal firewall program. A personal firewall program, among other safety features, helps you detect the presence of an intruder program by alerting you every time one of your programs — or, more importantly, a program being controlled by a hacker or zombie PC — tries to connect to services or locations on the Internet that you don’t normally frequent.
Most antivirus software now blocks spyware as well, but you can also avoid it by not clicking unknown links or installing unknown software from the Internet. This includes that link saying your computer is already infected — it isn’t now, but it will be after you click the link.

And don’t forget to update your software, either! Privacy and security problems are most likely to show up in operating system, e-mail, browser software, and other communications software, such as instant messenger programs. The good news is that the media is very good about covering stories about privacy holes in software, so you can be sure that if one of the programs you use has a problem, you’ll hear about it. When you do, hightail it to the web and download the security fix. Operating systems and apps usually do a good job of letting you know when updates are ready, but it’s also good to be proactive.

Mobile devices don’t suffer as much vulnerability as PCs because they operate in a more closed environment and often use a locked operating system. However, just because it isn’t a common occurrence doesn’t mean it hasn’t happened. Both major app stores (iOS and Android) have seen instances where potential malware found its way into downloadable apps. Both services were able to eliminate the threats remotely, but you still need to be aware of what you install on your device, and which links you click (even in SMS messages or apps like Twitter or Facebook). Consider using antivirus software for all of your devices — even your smartphone and tablet — by downloading antivirus apps from the app store on your device.

**Recognizing Scams**

Keep your eyes open and your head on a swivel, and you’ll avoid a lot of what the Internet has to throw at you. This section looks at common scams and how to avoid them.

**Gone phishing**

Eventually, you’ll receive an e-mail that says it’s from your bank or from eBay, PayPal, or a similar website announcing a problem with your account. Invariably, the e-mail offers a handy link to click, saying that you must enter your username and password to set things in order.
Don’t do it, no matter how realistic the e-mail and website may appear. You’re seeing what happens in an ugly industry called phishing. Fraudsters send millions of these messages worldwide, hoping to convince a few frightened souls into typing their precious account name and password.

How do you tell the real e-mails from the fake ones? It’s easy, actually, because *all* these e-mails are fake. Legitimate finance-related sites may send you legitimate history statements, receipts, or confirmation notices, but they will never, ever e-mail you a link for you to click and enter your password.

If you’re suspicious, visit the company’s real website by typing the web address by hand into your browser’s Address bar. Chances are good that the real site won’t list anything wrong with your account.

Many of the scams discussed in the following sections are types of phishing scams.

**Looking for love**

Romance scammers cruise online dating websites such as Match.com or eHarmony.com. They post hundreds of messages, looking for responses from people eager to meet that special someone. After weeks of online wooing, the scammers ask the victim to wire money so they can come for a visit or to deal with a personal emergency. The vulnerable victim willingly forks over the money to the new love interest, who then disappears from the site. The average financial loss from these schemes is more than $10,000 per person.

**Health care scams**

Here’s how this scam works: You receive an e-mail offering free medical supplies or warning that you may lose Medicare benefits. Some of these scams have a form that asks for personal information such as your full name (including your middle name), birthdate, address, occupation, marital status, and telephone number, as well as sensitive medical history data. The result can be old-fashioned financial fraud or a specialized variant, medical identity theft, in which impostors get health care services under your name, leaving you with the tab.
To avoid becoming a victim, don’t give out this information. Just delete the e-mail.

These scams have been on the rise because they play to the fears about rising health care costs and the changing policies resulting from the Affordable Care Act.

**Bogus charities**

You receive an e-mail from a charitable group soliciting a donation, and asking for a reply by e-mail or providing a link to a website. Be careful. This tactic has been used as a ploy to get your credit card number and expiration date, or a personal check.

You can take steps to ensure your donation is going to a legitimate charity. For instance, go online and look up the charity, rather than using the link in an e-mail solicitation. The website will have all the contact information to make a donation.

Don’t stop donating to charities — just don’t give out your personal information to strangers on the telephone or by e-mail. In most states, the charitable organizations must be registered with the state attorney general, so check whether the charity is legitimate before you donate.

**Bogus invoices**

This scam involves phony invoices made to look like the real thing. This may be the newest trend to garner personal information from you. We’ve received some bogus invoices via both e-mail and U.S. mail. One telltale sign of a bogus invoice is the lack of a phone number for an alternative contact method.

To comply with U.S. Postal Service regulations, solicitations are required to have the wording in the following example — the disclaimer is easy to spot in the postal mail, but you don’t always see it in e-mail messages:

**THIS IS NOT A BILL. THIS IS A SOLICITATION. YOU ARE UNDER NO OBLIGATION TO PAY THE AMOUNT STATED ABOVE UNLESS YOU ACCEPT THIS OFFER.**
The wording is required to be near the top of the invoice in capital letters, in bold type, and at least as large as the letters on the solicitation. Often the disclaimer is overlooked or misunderstood. The idea is to get you to pay for something you didn’t order. Sometimes the scam is used to solicit credit card information.

Don’t respond to invoices that don’t have phone numbers on them. If you didn’t order what’s stated in the invoice, simply ignore it.

**Phony investments**

In the phony brokerage-firm scam, the thieves set up a website using the name of an actual brokerage firm, but they use a different address. Then they craft and send a spam e-mail. The e-mail usually trumpets upcoming “hot” stock to entice you into visiting its website. On the site, you provide your credit card number and other personal information to purchase the “stock.” At the time of this writing, it isn’t clear whether the scam is being perpetrated to garner personal information to use in further identity theft frauds or whether it’s collecting money for phony stocks.

In any event, don’t purchase stocks from unsolicited e-mails; it’s probably just a ruse to get your personal information, or it’s not a good tip anyway. If you’re interested in buying stock, contact a brokerage firm near you and set up a face-to-face meeting in its office.

**Temporary account suspension**

The scam touting a temporary suspension of your account is set up either in an e-mail or a telephone call. The thieves use the scare tactic that your bank account (or online payment or online auction account) has been suspended. The e-mail sender or phone caller claims that the bank is reviewing all of its accounts to eliminate waste and fraud. You’re then requested to visit the “company’s” website to provide the information necessary to review your account and to make sure that the information on file is correct. The information they ask for is the usual: full name, account number, ATM or debit card number, and PIN. The e-mail sender or phone caller goes on to say that if you don’t provide the information, your account will be permanently canceled.
You know what happens next! You become the victim of identity theft. Don’t provide the information. Contact your bank instead.

**Job scams**

Several times a week, you may receive e-mail invitations to work at home or as a shipping clerk or to transfer funds for various companies. These are usually scams. If you fall for them, you could lose money and put your personal information — such as your address, SSN, and bank account number — into the wrong hands. Don’t apply for unsolicited job offers, even if the e-mail states that your information was garnered from a job website.

Most of these bogus job scams suck you in with the promise of thousands of dollars for working a few hours a day from your home. Some of the job scams can land you in trouble with the law because the activities you’re asked to perform involve money laundering and repackaging of merchandise bought with stolen credit cards.

You can find out whether an e-mail job offer is a scam by going to [www.scambusters.org](http://www.scambusters.org). That website describes numerous scams, and you can search by the type of scam.
Chapter 3
Password Secrets

In This Chapter
▶ Picking a quality password
▶ Storing and remembering your passwords
▶ Understanding password vulnerabilities
▶ Using encryption

Unless you’re off the grid in the Montana woods or working with extremely secure biometric sensors on a top-secret government project, you deal with passwords every day.

Some computers already allow you to access your information with fingerprints and other biometric scanners. However, those methods usually work for hardware only. If you want to get anything done on the Internet, you need passwords — many, many, many passwords. This chapter takes a look at all those passwords (and security questions) and what you can do to make them less “hackable.”

Where Do I Use Passwords?
The easy answer to this question is, everywhere. It seems like everything online requires a password of some sort. From accessing your computer to getting your e-mail to viewing your bank records, you identify yourself with a password. The questions you should ask are along these lines: How long should I make the password? What characters should I include in that password? Should I use a password or a passphrase?
Choosing and Protecting Passwords

When you set up an account on the Internet, you have to set a password, which is the keyword you type to confirm your sign-in along with your user ID. Passwords are used not only in e-mail but also on almost every website you become a member of, and with many apps and devices. If you have a strong password, hackers will pass by your account and attempt to hack an easier target. In this section, we tell you how to make wise password choices and also how to protect those passwords after you’ve chosen them.

Picking a strong password that isn’t easily cracked by thieves is not as thought-free — but is twice as important — as it may seem. Whoever has your password can (in effect) be you anywhere on the web — posting comments, sending spam e-mail messages, and leaving dangerous messages (which can range from pranks to scams or worse) for others to see. Basically, such an impostor can ruin your online reputation and possibly cause you serious financial grief.

What goes into creating a foolproof strong password? You could slam your hands into the keyboard and go with those results, but odds are that you wouldn’t remember what you entered. And you’d hurt your hands, but that’s a different concern. Take a look at these more practical solutions:

 ✓ Don’t pick obvious passwords. Don’t use your first name or last name or your dog’s name or your spouse’s name or your birthday or your birthday backward or common words in English or any other common language. Someone who really wants to get access to your computer already knows to try this kind of personal information first. If you aren’t feeling creative or otherwise up to the task of inventing random passwords, you can find freeware and shareware password-generating applications by visiting CNET’s Download.com (http://download.cnet.com) and searching for password.

 ✓ Create longer passwords. The longer the password, the better — 10,000 combinations are possible with a 4-digit password. The number of possible combinations for a 5-digit password is 100,000 (or 10x10x10x10x10). For a 6-digit password, 1 million combinations are possible.
✓ Use both numbers and letters. Throw a few letters into the password, and you really make things complicated. A 4-character password consisting of both letters and numbers has 1,679,616 possible combinations. (That’s 10×26+10×26×10+26×10+26, for you math fans.) For a 5-character password, 60,466,176 combinations are possible.

✓ Throw in a few symbols — like $, &, % and * — just to make guessing your password even harder. Sometimes a software program or your operating system doesn’t let you use nonalphanumeric characters, but if your system lets you, you certainly should! (This advice applies to your Internet service provider and other online passwords as well.)

Just remember, with good password-cracking software — available for free from the web, of course — it takes only about a minute for a hacker to crack your password and potentially access any data they want to.

With any password, you should follow these common sense rules to protect your privacy:

✓ Don’t give your password to anyone — it’s like giving away the keys to the front door of your house.

✓ If you even suspect that someone has your password, immediately change it.

✓ Change your password every few months just to be on the safe side. Maybe even rotate a group of passwords over the various accounts you use.

For a truly strong password, tie four random words together like “Davescatsniffsglue” and use some substitute characters, such as “Dav3sc@tsn1ff5glu3”. Also, use as many characters as you can. Windows 8, for example, allows a password up to 16 characters long. Use the maximum number of characters allowed.

Storing and Recalling Passwords

It would be impossible to remember all your passwords. Many websites ask you to enter a username and password. If you’re buying an item from an online store such as Amazon.com, you
create an account with a username and password that you enter every time you want to buy something. Amazon.com remembers your name, address, and credit card information as part of your account, so you don’t need to enter it every time. If you want to read The New York Times online at www.nytimes.com, you create an account with a password, too. The account remembers what kinds of news you’re interested in reading. After you use the web for a while, you pile up a heap of usernames and passwords. And widespread use of smartphones and tablets means that passwords are even more ubiquitous. Many apps require login, either for security or for data syncing. Even your device itself may require a PIN, password, or some identifying action to gain access.

When a web page asks for a username and password, your browser may pop up a little window that offers to remember the username and password you enter, or the question may appear just above the top edge of the web page. If you click Yes, the next time you arrive at the same page, your browser may fill in your username and password for you.

Depending on who else has access to your computer, you might let your browser remember passwords to only those accounts that don’t involve spending money or revealing personal information. For example, if you have an account at a celebrity fan site that enables you to participate in online discussions, the danger of having someone break into this account is a lot less daunting than the thought of someone hacking into your online bank account. Unless your computer is in a physically secure place, don’t let your browser remember passwords that have any real power.

As we mention earlier, the standard advice is to construct passwords from a mixture of letters, numbers, and symbols; to assign a different password to every account; to never write down passwords; and to change them every few months. Most people have dozens of accounts and ignore this advice because only a truly unusual person can remember dozens of different random passwords and which account goes with each one.

We suggest a compromise: Make up one good password to use on all your low-risk accounts — accounts in which letting someone else gain access has little consequence, such as online newspaper subscriptions. Use different passwords for
the accounts that truly matter, such as online banking. Writing down these passwords and keeping them in a safe place is better than picking a password that’s easy for someone to guess. Don’t list your passwords on a sticky note stuck to your computer’s monitor.

If you write down your passwords, secure the paper — and we’re talking under-lock-and-key secure, not just in-the-car secure. Also, remember that you and only you should have access to that record.

You can also use password management programs like 1Password (https://agilebits.com/onepassword), LastPass (https://lastpass.com/index.php?fromwebsite=1), or RoboForm (http://www.roboform.com/download) to manage all your browser-based passwords securely. These programs encrypt your passwords and restore them when needed, locking them away when not in use. Do your research and stick with the big names on this one. If you can’t find any reviews or respected authorities talking about and endorsing the app, it isn’t good enough for you. Word spreads quickly about bad software, so go with only those that are well known.

Understanding Password Vulnerabilities

Getting into your home computer shouldn’t require a blood test and a waiting period, but you can’t let just anybody use your information, either. At this point, computer login services seem to have settled on requiring a user ID and a secret password, which are usually adequate. However, passwords give a false sense of security. The bad guys know this and attempt to crack passwords as a step toward breaking into computer systems. Common words or combinations of characters just make it too easy. As much of a pain as it is, using a unique string of letters, characters, and numbers is better than using a common term you can easily remember.

One big problem with relying solely on passwords for information security is that more than one person can know them. Sometimes, this is intentional; often, it’s not. The tough part is that there’s no way of knowing who, besides the password’s owner, knows a password.
Knowing a password doesn’t make someone an authorized user.

Even with good passwords, hackers can find ways to get this information and access your systems. If your company doesn’t make you choose a strong password or store that password correctly, whatever password you do use isn’t all that secure. And now that more and more employees can work remotely, you don’t always have the security of a private office.

Using Encryption

Encrypt a piece of data and suddenly it doesn’t mean anything to anyone any more — except for you and anyone else who has your password or key. Simply put, encryption scrambles data. So the fear of data being stolen or intercepted is gone because your data in the wrong hands is just gibberish.

If you use encryption software to encrypt your list of passwords for safekeeping, you have to remember only one password: the one for your encryption software!

If the benefits of glorious gobbledygook sound good to you, here’s how to put encryption to work on your own data:


✓ Encrypt files on your hard drive. They’re your files, darn it, and you don’t want anyone else reading them. The trick, then, is to encrypt them so that if someone without the password does open your files, all he sees is something like this:

```
dfjkl;sdjfk;l;sdjfk;l;sdjwe
rtsdjk;l;sdjk;l;sdajkl;dfgweruioerwjio
or sdfsdk;l;weruieruijksdflnjkku90wer
or xcvnm$9ke*sd893
```

Lots of freeware and shareware programs are available that enable you to encrypt your files. To find them, browse to Download.com and search for encryption.
Your computer operating system can also provide encryption options. Windows users should look up BitLocker (http://windows.microsoft.com/en-us/windows-8/bitlocker), and Mac users can rely on FileVault (http://support.apple.com/kb/HT4790).

**Appreciating Password Enhancements**

When you want to keep your information truly secure, you can look into the options in this section to safeguard your passwords. The problem is that you can’t really force accounts to use these measures. If a provider offers these features, by all means take advantage of them! If the provider doesn’t give you these options, you can still use a good password and keep your information as secure as possible. But you might encourage the provider to add these services as soon as possible (or look for a different provider):

- **Two-factor authentication:** This process requires you to log in at least once to an account using a back-up code in addition to using your password. This may sound complicated, but two-factor authentication helps keep your passwords truly private. Unfortunately, not all services require this feature. But Google does, so it’s a good example. When you create a Google account, you can specify a mobile phone number to receive a text message when you try to log in to the account from an unfamiliar computer or device. Google sends a text message to the number with a code, and you must enter that code to access the account. An intruder is less likely to have your password and access to your phone, so your information remains safe. If a service offers two-factor authentication, use it!

- **Passphrases:** Just as hackers have to work a little harder to guess longer passwords, they have to work that much more with passphrases. You have to spend a little more time typing “The quick brown fox jumps over the lazy dog” than you do “kZx43$,” but you keep your account far more secure.

  Don’t use “The quick brown fox jumps over the lazy dog” as a passphrase unless you want your account hacked by those persons who took typing classes in the mid- to late 20th century.
✓ **Captcha:** Never mind what captcha stands for — the effect is that you have to squint at a distorted picture of a series of characters and type those characters into a text field. This method prevents automated hacking attempts from gaining access to your account, presumably because only a human can discern what those characters are. Or they just frustrate us — one of the two.

✓ **VPN connection:** No matter what security method you use, it’s always safer over a *virtual private network* (VPN). Most workplaces offer them, and you can buy commercial alternatives as well. These connections encrypt all traffic to and from your device, making it all the more safe for your use.

## Answering Security Questions

Security questions have been around forever. Think of the cliché from war movies where a couple of GIs ask an approaching soldier who won the World Series last year. On the Internet, these questions get a lot more personal, but the purpose is the same: to identify who you are in case a provider needs more verification (to reset a password, perhaps).

These security questions can range from your mother’s maiden name to your favorite sports team or color. When you first create an account, you’ll provide answers to the security questions, and the provider will ask for the answers when necessary. If the answers match, you’re good. If not, you don’t get access. Therefore, these questions tend to be precise (What was the name of your first pet?) rather than nebulous (How do you feel today?).

However, you *don’t have to answer correctly!* You can select a wrong answer when you initially set the security question and remember to give the wrong answer every time. For example, tell the service that your favorite team is the Cleveland Browns. Nobody ever guesses that.
Chapter 4
Risk-Free E-Mail

In This Chapter
▶ Creating safe e-mail aliases
▶ Dealing with spam
▶ Spotting common e-mail scams
▶ Dealing with phishing e-mails

To a great extent today, e-mail messages have replaced letters, providing an almost instantaneous way to stay in touch, conduct business, and exchange documents. However, e-mail carries certain risks that you should be aware of.

✔ An e-mail may contain links or files that, if opened, can place malicious code on your computer or cellphone.

✔ **Spam** is generally e-mail advertising for a product that arrives unsolicited from somebody you don’t know. Spam can be a nuisance, and can also lead to more serious issues.

✔ Spam becomes a **scam** when criminals use the e-mail to commit fraud. It may be a financial scam (called **phishing**) where they make the e-mail look like an official notice of some kind to lure you into revealing financial information that they can use to steal your money or identity. Or it may be to get you to click on a link to place malicious code on your computer to steal all your information. These scams come in several varieties, but they share certain characteristics that we explore in this chapter.

Luckily you can use safe e-mailing practices, filters, and your smarts to avoid spam and malware, and to spot common scam characteristics so you can avoid becoming a victim. In this chapter, you discover how to e-mail safely.
Following E-Mail Safety Basics

Adopt the following e-mail practices to keep you safer every time you e-mail:

- **Don’t share.** Never share sensitive personal information in e-mail, such as passwords, Social Security numbers, and credit card numbers. Even if you e-mail this information to a known person or business, it can be intercepted along the way.

Pay attention if you use an automatic e-mail signature. This handy feature automatically provides whatever signature information you choose to share. Many people include their full name, address, and phone number in their signatures. But if it’s inserted in all your e-mail responses, you might be sharing more information with people you don’t know than you intend to, especially if your friends forward your e-mail to others.

- **Consider who you want to receive e-mail from.** Just because someone sends you an e-mail doesn’t mean you need to read it or respond to it. You can set up your spam filters to be fairly restrictive and then check your junk mail folder periodically to see whether something important accidentally got blocked. (If you aren’t sure how to do this, consult the Help documentation for the e-mail program you use.)

- **Think twice before you open attachments or click links in e-mail.** If you don’t know the sender, delete the email; if you do know the sender but weren’t expecting an attachment, double-check that she actually sent the e-mail. If your friend didn’t send you the attachment, delete the message. If her computer is infected with malicious code, it may automatically send you e-mails (without her knowledge) with links or attachments in an attempt to infect your computer as well.

- **Talk to people you e-mail with about their online security.** If they don’t protect their computers from viruses, spyware, and other malicious code, they put you at risk every time they send something to you.

- **Report offensive, inappropriate, and illegal material sent via e-mail to your Internet service provider (ISP).** If the content is illegal, you should also report it to your local law enforcement agency.
✓ Be cautious about meeting online contacts in person. You may know certain people only through e-mail or contact on a website. Just remember that everything someone tells you about himself and his motivation for meeting you may be completely true — or completely false. If you decide to meet someone in person, don’t go alone. Make sure others know where you’re going; meet in a very busy, public place; and keep your cellphone handy.

✓ Consider what you’re saying and sharing in e-mail and how you’d feel if the information were shared with someone other than the recipient. Anything you say in e-mail could be forwarded to others or monitored by employers or family members.

Avoid typing sensitive information into public computers such as those found in libraries or Internet cafés. Sensitive information includes your name, phone numbers, account numbers, passwords, and home or e-mail addresses. These computers may be infected with spyware that records your information and sends it to a criminal. Never select the feature that automatically logs you on to e-mail when you start the computer, and don’t select a Remember My Password option when using a public computer. If you do so by mistake, use the Forget My Password option on the login screen for that account to reverse the action.

Creating Safe E-Mail Aliases

Your choice of an e-mail alias can provide as little or as much information about you as you choose to share. An e-mail alias like JackStanfield@hotmail.com exposes your full name. This may be exactly what you want, or you may not want to give away any personal information. Just remember that whatever information you provide in your e-mail address, many kinds of criminals — whether their intent is to cause financial, emotional, or physical harm — can see it, in addition to those you trust.

Consider the exposure in this e-mail alias: SusieDoe_64_small_town@google.com.au reveals enough information for someone to find Susie — her name, age, and small town in Australia. And flirtatious names like sexyOver50 may cause unwanted attention and expose you to greater risk.
If you want the safest personal e-mail alias or nickname (versus your work e-mail, over which you may have little control), don’t provide identifiable information, such as

- **Names:** Don’t provide first, middle, or last names. If your e-mail provider displays your full name next to your alias by default, be sure to read the next section to change settings or else avoiding the use of your name won’t do you any good.

- **Location information:** Don’t provide city, town, country, or region, such as Northwest. Don’t give away your employer in your personal e-mail alias.

- **Sexual or physical suggestion:** Certain words such as *hot* and *sexy* let others know how you want to be perceived, whereas words like *snuggly* and *lonely* suggest an interest in intimacy that criminals can take advantage of.

- **Work descriptor:** Don’t announce, for example, that you’re a teacher, an engineer, or a dentist or that you’re retired, and don’t give a description of your place of employment.

- **Emotional vulnerability:** Words such as *sad*, *grieving*, *lost*, and *lonely* place you at risk; there’s always a criminal waiting to be your “best friend.”

- **Risk behaviors:** Names that speak, even in fun, of drug use, criminal activity, or violence may attract the wrong kind of person.

- **Ethnic identifiers:** These may increase the risk of hate crimes, or they may help identify you — for example, *N8tive* (native), or *mxed* (mixed).

- **Hobbies or sports:** An unusual sport such as polo or barrel riding, sports that imply a specific socioeconomic bracket, or sports that take place in only a few locations (skeet shooting or bull fighting, for example) are more identifying than baseball or soccer. Criminals can use such interests to make a personal connection with a victim.

Employers may have defined domains (@company.com) and assigned protocols for your name — even using your full name. It’s important in these cases that you limit the additional pieces of personal information you associate with that account. For example, you may provide your work phone number in your signature but avoid including a personal cellphone number or your personal e-mail account.
Hiding Your Name in E-Mails

Some e-mail services automatically include your full name as well as your e-mail alias to everyone you send e-mail to. If this isn’t what you want, you need to find out whether this is happening. Send yourself an e-mail and look at who it’s from. If your name appears there, take steps to remove this information.

Think about it: Your last name and an online directory search may be all it takes to locate your family, find your phone number, learn the value of your home, and more. Check your e-mail provider’s Help topics to get steps for this procedure. (For Windows Live Hotmail and Yahoo!, the steps are at http://ilookbothways.com.)

Opening an Attachment

You may receive e-mails with attachments. Be very cautious about opening these if you don’t know the sender — or if you don’t expect an attachment from someone you do know. Some malware programs can copy your e-mail contacts and send out messages that may look like they come from you. It’s for that reason that, even if a message with an attachment appears to have come from somebody you know, you shouldn’t open the attachment unless you’re expecting it — or unless you verify with the sender that the attachment is legitimate. Also, always be extra careful about opening an attached file with a file extension of .exe. This is an executable file, which is the file format that most malware takes.

If you want to open the file or run an executable file (such as an installation program for software that initiates the installation), click the Open or Run button. (The choice varies depending on the type of file.)

Be aware that clicking either Open or Run is an extremely high-risk action. If you aren’t 100 percent sure that what you’re opening is an installation program for a legitimate piece of software, don’t proceed.
Managing Spam

Aside from being the name of a popular, canned, pseudo-meat product, *spam* in the e-mail world is junk e-mail sent in bulk to recipients who haven't requested it. People usually get spam from senders they don't know. Spam can be transmitted over any Internet-connected device (such as a computer, smartphone, or tablet). It's a cheap way to market products or services, but it’s illegal in many countries.

Though ISPs are making serious efforts to block spam e-mail, determined spammers are making equally serious efforts to find ways to keep filling your inbox. They constantly evolve new methods of fooling the anti-spam filters. Here's some advice about how to avoid and deal with spam:

- Understand your e-mail provider’s antispamming features, and use its settings to flag spam or to put it in a separate junk mail folder.
- Review the junk mail folder periodically to make sure legitimate e-mail hasn’t been placed there. Then delete the spam e-mails without opening them.
- Stay up to date on spam tactics. (Visit [http://ilookbothways.com](http://ilookbothways.com) or sites such as [www.snopes.com](http://www.snopes.com) for the latest information.) When in doubt about the origin or intent of an e-mail, delete it.
- Always have strong antispam, antivirus, and antiphishing tools installed on every computer you own, set these tools to update automatically, and use settings in your e-mail program to block spam.

Using Spam Filters

Spam filters identify spam and keep it out of your inbox. Most e-mail programs have built-in filters that route spam to a Junk folder or immediately delete it.

Most spam is easy for filters to identify. Filters can flag known bad senders or spot keywords in the subject lines, such as *Viagra* or *sex*. But no matter what filter level you choose, you
should periodically check your Junk mail folder. Spam filters aren’t infallible, and legitimate e-mails can end up in there by mistake.

Consult the Help documentation for your e-mail program to learn how to apply the filters.

Report spam to your e-mail provider by whatever method it provides. By reporting spam, you can help your e-mail provider more accurately track and reduce spam for everyone.

Filing a Spam Complaint

The United States federal CAN-SPAM Act of 2003 went into effect on January 1, 2004. The CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing) was created by federal lawmakers as a way to reduce spam. The CAN-SPAM Act states that it “preempts all state law that regulates commercial e-mail except to the extent that state law prohibits falsity or deception.”

The federal statute

- Requires commercial e-mail senders to provide recipients with the ability to opt out of receiving more e-mail
- Requires e-mail to be identified as advertisements or commercial e-mail where applicable
- Requires sexually oriented e-mail to be labeled as such on the Subject line
- Requires the physical address of the sender to be included in the e-mail
- Creates criminal penalties for those who violate substantive provisions of the law

To file a complaint under the CAN-SPAM Act, e-mail details to the FTC at spam@uce.gov.

The FTC also provides more detailed information about spam issues and the CAN-SPAM law on the FTC website, www.ftc.gov/spam.
Recognizing Fraud and Scams

As in the offline world, the Internet has a criminal element. These cybercriminals use Internet tools to commit the same crimes they’ve always committed, from robbing you to misusing your good name and financial information. Know how to spot the types of scams that occur online and you’ll go a long way toward steering clear of Internet crime.

Think before you click. Doing so will save you and others from scams, fraud, hoaxes, and malware. For example, before you click a link that comes in a forwarded e-mail message or forward a message to others, ask yourself these questions:

- **Is the information legitimate?** Sites such as www.truthorfiction.com, www.snopes.com, or http://urbanlegends.about.com can help you discover whether an e-mail is a scam.

- **Does a message ask you to click links in e-mail or instant messages?** If you’re unsure whether a message is genuinely from a company or bank that you use, call the company, using the number from a past statement or the phone book.

  Don’t call a phone number from the e-mail; it could be fake. To visit a company’s or bank’s website, type the address yourself if you know it or use your own bookmark rather than click a link. If the website is new to you, search for the company using your browser and use that link to visit its site. Don’t click on the link in an e-mail, or else you may land on a site that looks right — but is just a good fake.

- **Does the e-mail have a photo or video to download?** If so, exercise caution. If you know the person who sent the photo or video, it’s probably fine to download, but if the photo or video has been forwarded several times and you don’t know the person who sent it originally, be careful. It may deliver a virus or another type of malware to your computer.

In addition to these questions, if you decide to forward (or send) e-mail to a group, always put their e-mail addresses on the Bcc: (or Blind Carbon Copy) line. This strategy keeps everyone’s e-mail safe from fraud and scams.
Avoiding the Latest E-Mail Scam of the Day

E-mail scams are typically low-value, high-volume crimes where the cost to a given consumer is comparatively low, but large numbers of victims mean that the money quickly adds up for the criminals behind the scam.

One way that consumers trip up relates to the relevancy of the scam’s topic. E-mail scammers are smart about making their scams look current, because people are much more likely to fall for scams related to topics already on their minds. For example, Valentine scams circulate around Valentine’s Day. Last year, a Valentine scammer e-mailed messages with titles including “In your arms,” “Sending you all my love,” and “I love you because . . .” These have short messages and links that you’re encouraged to click. Clicking the links downloads malicious software onto your computer.

The Subject lines of e-mail scams morph constantly. Also, around any holiday, be on the lookout for e-mail messages offering “great deals” on flowers, chocolates, dinners, and other products. If you aren’t sure that a store is reputable, don’t go there. When you’re in tax season, tax-related scams abound, including scams about being audited, getting tax rebates, or offering tax-filing assistance. And the list goes on. There’s literally a scam for every occasion.

Avoiding Phishing

Phishing scams are attempts to trick you into divulging sensitive personal information that allows somebody to steal your identity or empty your bank account.

Don’t be fooled by phishing. Be very skeptical if you receive an e-mail that looks like it’s from your bank or broker or another trusted company but asks you to verify or reenter sensitive personal or financial information through e-mail, a website it directs you to, or a phone number it provides. It’s quite likely a scam.
Look for these telltale signs to spot a phishing e-mail:

- You don’t know the sender.
- The wording in the e-mail includes typos or is not grammatical.
- You’re asked to provide information such as an account number, phone number, or Social Security number.
- The e-mail address is odd-looking or lacks a business name. Legitimate businesses have their own domain names (such as comcast.com or disney.com).
- You’re asked to click a link to respond or take an action. If you check the properties of the link by right-clicking it and choosing Properties, you find that the address is bismark.net, not Amazon.com.
- You’re told that you must click the link and provide information to get access to your account.
- You’re told not to reply to the e-mail because it’s an automated e-mail and won’t be answered. You’re instead urged to log in to your account (using the link it provides).

If you receive a phishing e-mail, take these precautions:

- Rather than click the links in the e-mail, use your favorite search engine to find the website for the company that sent the e-mail or locate that information on your statement.
- Contact the institution using a phone number from a statement or type a company website address in your browser to go to its site and ask about the communication.
- Report the scam to your e-mail service provider.
The greatest gift the Internet gave to the world might be the ability to locate and purchase just about anything in the world you might want. Point, click, type a few numbers, and you’re ready to go! That said, you have to be sure exactly who is taking your money and whether that person will actually send you what you’re expecting (such as a real iPad instead of just the box that once contained an iPad). This chapter helps you identify authentic websites and ensure that your financial transactions are conducted with the highest possible security.

Vetting Websites Critically

Look around and be choosy. If you walked into a restaurant and saw a dirty floor and signs of mice or you were assaulted by an unpleasant odor, I hope you would turn around and walk out. If you’re smart, you apply the same principle when shopping and banking on the web. Look around before you whip out your credit card. Ask yourself, “Does this site look like somebody put it up over a weekend? Or does it look like someone worked really hard to make my shopping experience a positive one? Has the company successfully instilled in me a sense of confidence and trust?” If not, it’s time to go shopping someplace else.
Just as you can’t judge a book by its cover, the legitimacy of a website is hard to gauge just by looking. If you see signs of poor quality, you may want to consider moving along. If it sounds too good to be true — you already know what comes next.

Use the power of the Internet to investigate. Just because you’ve never heard of a website doesn’t mean that it isn’t a good company. Look up reviews on your favorite search engine or check social media. Chances are, if something went wrong, people are talking about it.

**Considering Online Versus Offline Banking**

Online banking may still have a few issues here and there, but for the most part, you can interact with your financial institutions online with no problem. And, as evidenced by the recent compromising of the accounts of hundreds of thousands of shoppers at several established and respected retail stores, your information can be compromised whether you’re shopping on the Internet or at a bricks-and-mortar store.

Consumer-facing institutions such as those companies, both online and off, have taken great pains to ensure the safety of your (and their) money. But just as with a bank, when a company has money — or the credit card numbers for lots of shoppers who have money — the bad guy wants it. And retail stores aren’t alone: Institutions from governments to universities and power companies are the targets of hacks almost constantly. Twitter, Facebook, and Google+, too, are all targets of hackers due to the wealth of personal information and access they can provide to those with ill intent.

Here are a couple of ways to make sure that your online banking transactions are as safe as possible:

✔ **Use encryption.** Make sure that both your browser and your bank’s website use 128-bit encryption, which, by some estimates, is so safe that it would take more than a trillion years for a hacker to crack using current technologies.
How will you know whether your browser offers 128-bit encryption? Most browsers tell you. For example, Microsoft Internet Explorer has an About Internet Explorer option on the Help menu. Choose that option to see which version of the browser you’re using, and in most cases the information includes Cipher strength, indicating the number of bits used for encryption.

✓ Look for a secure server. This advice goes hand in hand with ensuring 128-bit encryption, but the secure server gives you a visual clue that it’s working. Look for the locked padlock icon on your browser and the addition of the letter s to the http — as in https — at the beginning of your bank’s URL.

✓ Ensure your bank is insured. Is this bank insured by the Federal Deposit Insurance Corporation (FDIC)? To be sure, check out the FDIC website at http://research.fdic.gov/bankfind.

✓ Get it in writing. Check your bank’s website for a written guarantee that protects you from losses from fraud that may result from online banking. You’ll be able to support your case more easily if you have printed copies of all your online transactions to prove that what you say is true.

Evaluating an Online Shop

Here are some questions to keep in mind when you’re shopping online. Astute shoppers will notice that many of these questions are the same ones to keep in mind wherever you’re shopping:

✓ Can you find the appropriate digital certificates indicating that the website is authentic?

✓ If you’ve shopped at this site before, do you regularly receive e-mail confirmation of your purchases?

✓ Does the website provide a clear and complete privacy policy?

✓ Are the descriptions clear enough so you know what you’re ordering?

✓ Are the prices competitive with other online stores and with mail-order and regular retail?
Does the store have the products in stock, or does it offer a firm shipping date?
Does the store have a good reputation?
Does the store have a clearly written privacy policy that limits what it can do with the data it collects from you?
Can you ask questions about your order?
How can you return unsatisfactory goods?

Guarding Your Card Online

Shopping the web is probably not as dangerous as trying to find a parking space at the mall 45 minutes before closing time on Christmas Eve. Simply follow the common sense advice in this section to protect your card online.

Ordering stuff without sharing your primary account information

Purchasing merchandise online is incredibly easy, but you must protect yourself. Here are some alternatives to using your own bank account or card on a shopping site:

Use a pre-paid credit card for online purchases. You can get a prepaid credit card almost anywhere these days — the mall, your bank — and you can fill them up with only a limited amount of money in case the number is stolen. If it is stolen, you haven’t lost your real bank card number.

Use a stored value card. This is similar to a prepaid phone card. You purchase the card with a certain dollar amount and each time you use it, the purchase amount is subtracted from the balance. For example, you could buy an iTunes card and use it for your iTunes purchases, or you could buy a Visa prepaid card and use it for everything else.

Use an online payment service. Through this service, you can set up an account and make purchases drawing from that account. For example, PayPal is one of the most popular and trusted online payment services.
Embracing safe shopping practices

Follow these guidelines to protect your accounts when you’re shopping online:

✔ Use the latest Internet browser. The browser allows you to navigate the Internet and provides encryption, which scrambles data sent to a server to protect it. When you use the most recent browser version, you’re also using the latest encryption version.

✔ Use only one credit card (or a debit card that’s not attached to your primary savings or checking account) to make purchases on the Internet. This way, you can track your purchases and activity on the card more easily. This is a good way to keep a record of all your Internet transactions to help ensure accuracy of your card’s charges. If the card is compromised, you can cancel it and get a new one. These days, online sites request the security code to complete the transaction, just as it is for phone orders. Merchants ask for the security code to help protect them from fraudulent charges, and the code also helps protect you because the identity thief has to get the code to complete the transaction.

✔ Don’t supply your password or ID online unless you know who you’re dealing with, even if your Internet service provider (ISP) asks for it via e-mail. This request is a scam and is used by identity thieves to collect personal information.

✔ Don’t store your credit card online with a service. It’s awfully convenient to store a credit card or two on Amazon or iTunes to facilitate quick purchasing. And the services want you to do it — that’s why they make it so easy! Just click the button and it’s yours! But that means that anybody with access to your account can just as easily get the information (and get the product shipped to them, of course). If you’re really concerned about keeping this information safe, refuse to let these services store any credit card information. This policy makes online shopping a little more inconvenient, and you’ll have to type in that information every single time, but the added security and peace of mind could be worth it to you.
Some banks such as Bank of America and Citi offer one-merchant unique credit card numbers. And even newer solutions come from the privacy company Abine (www.abine.com), which enables you to mask your real credit card number by giving you a fictitious number for transactions. You can even set a credit limit for each fictitious number.

By the way, that suggestion to never send information in an e-mail applies to Social Security numbers, bank account numbers, passwords, or just about anything else except for happy cat photos. Almost everyone loves happy cat photos.
Chapter 6

Ten Things You Can Do Today to Protect Yourself

The fact is, hackers are always trying to break down the security of personal and public security technologies that protect companies, governments, other organizations, and thus you and your data — and the bad news is that sometimes they succeed. The good news is that you can do lots of things today to make sure that your digital activities are as safe as possible.

If you’re an action-oriented person, this chapter is for you. Here we describe ten things you can do, starting now, to help you stay safe online.

Use Two-Factor Authentication

Use two-factor authentication where available, as discussed in Chapter 3.

WARNING!

Make sure to write down temporary codes for all services in case your smartphone is stolen, or else you may be temporarily locked out of all services that require you to have a smartphone to receive a text.

Stay Safe While Gaming

Make sure you’re using a reputable gaming site or software, and if you want to interact with other players but don’t personally know all of them, set up a safe profile with nicknames, usernames, and gamer tags that don’t identify you. Take care when chatting with other players: Do not give them your real
name, and do not buy gold offline from them. Just don’t trust them with any information at all by default until you have good, solid reasons to trust them.

If you’re into video chatting with other players, watch what appears in the field of view on your walls or bookshelves — anything they can see should be benign in nature in regard to identifying you. Even seeing religious books on your shelf might be enough to help identify what church you go to, and having your personal to-do calendar, appointments, or bills to be paid visible in the background is also a bad idea for obvious reasons.

Secure Your Public and Private Wi-Fi Connections

The three major types of wireless security are WPA, WEP, and WEP2. Use WEP2 because it’s the latest and most secure of the three. Use extremely strong passwords (see Chapter 3) and when in public, either don’t even mess with any secure data while on the public network or use smartphone tethering to give your devices access to a WEP2-secured connection. Public Wi-Fi networks are absolutely unsecure, so act as though a thief is looking over your shoulder in such places, because one may well be doing so.

Understand and Use Privacy Settings on Social Media Sites

Even if you select the Private setting on a social networking site or discussion forum, your profile settings are typically public. When you sign up for a service and provide the required information, selecting the private mode may not prevent others from viewing your photo, name, URL, city, state, and date you last logged in. Check your public profile after you sign up to see what’s exposed. If you’re not comfortable with the exposure, remove some information or close your account. The information can be used to help ID thieves, cyberbullies, scammers who pretend to share your interests, and other criminals.
Chapter 6: Ten Things You Can Do Today to Protect Yourself

Protect Devices with Passwords

It can be tempting to not require a password or PIN for your smartphone or tablet to more quickly get into it, but if your device is stolen, you may well regret not having protected it with a login password. Use a password or PIN on your devices for security.

This advice can be a lifesaver if you have children in the house: If you use a password for your device and require a password for purchases through your device’s online store, you don’t have to worry about games with in-app purchases racking up huge bills on your credit card.

Choose Carefully Whom You Share Personal Info with Online

The easiest way to protect yourself online is to never tell anybody anything. A pair of glasses and a cape might be helpful as well. Seriously, though, you’re going to have to share some information if you want to interact on the Internet. So you’re not looking for a secret identity as much as you’re looking for a trusted and limited identity. You want to share only the information necessary and with only those who really need it. So maybe you’re okay with giving your full name to a social network, but not to a site you’ve never heard of. And you’re okay with putting a PIN into a banking website, but you certainly wouldn’t post it on that social network.

Give Up On Safe Ways to Back Up Your Files Online

If you’re using cloud storage services such as Google Drive, Microsoft’s OneDrive, DropBox, or Apple’s iCloud, bear in mind that at present you can only protect that data from being seen by anyone other than that company and the government. Given recent revelations about the U.S. government’s National Security Administration having broken online encryption and gaining access to all major online services, including Google...
(and thus Google Drive), Microsoft (and thus OneDrive), and Apple (and thus iCloud), online backups really aren’t secure from everyone — only people outside of the government or that corporation. Some start-ups in other countries are capitalizing on “data not stored in America” at this point, but no major forerunners in the market are evident yet. To avoid losing valuable data to a data thief, you should know how to make backup copies of your files and folders on a recordable CD/DVD, flash drive, or portable external hard drive.

Consider storing the data in multiple geographical locations to avoid having a single copy be all that’s between you and having no data. A bank safe deposit box can be a secure second location, for example.

### Consider Location Settings on Devices

Be aware of the locations settings on your smartphone and tablet. Google and its Android operating system require location settings to be active to effectively get navigation, directions, and other local features. So does Apple, so no matter which device you have, if you’re going to use geolocation services on your devices, use strong passwords and encryption, and keep your device’s operating system up to date.

### Create a Google Alert for Your Name

Put a Google alert on your name so that if any new postings with your name show up in Google’s search results, they’ll let you know and you can assess the potential impact of the information, if any, immediately. Simply go to www.google.com/alerts to set up your alert request.
Surf Privately in Public

Remember to use In Private Browsing, Private Browsing, or Incognito Browsing features in Internet Explorer, Firefox, and Chrome, respectively. These features, which were built to ensure privacy, don’t remember (or offer to remember) passwords, usernames, or browsing history.

For additional privacy when browsing, consider the WhiteHat Aviator web browser (https://www.whitehatsec.com/aviator). WhiteHat Aviator includes a variety of built-in activated security and privacy safeguards.

Be sure to sign out of all websites when you’re on a public computer.
Publisher’s Acknowledgments

Senior Acquisitions Editor: Katie Mohr
Senior Project Editor: Sara Shlaer
Contributing Author: James Russell
Editorial Assistant: Anne Sullivan

Project Coordinator: Melissa Cossell
Cover Photo: ©iStockphoto.com