COMPUTER SECURITY FUNDAMENTALS

SECOND EDITION

CHUCK EASTTOM

Computer Security Fundamentals

Chuck Easttom

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Computer Security Fundamentals

ISBN-13: 978-0-7897-4890-4
ISBN-10: 0-7897-4890-8

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

Printed in the United States of America

First Printing: December 2011

Associate Publisher
David Dusthimer

Acquisitions Editor
Betsy Brown

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Keith Cline

Indexer
Brad Herriman

Proofreader
Debbie Williams

Technical Editor
Dr. Louay Karadsheh

Publishing Coordinator
Vanessa Evans

Book Designer
Gary Adair

Compositor
TnT Design, Inc.

Contents at a Glance

Table of Contents

About the Author

Chuck Easttom has been in the IT industry for many years working in all aspects including network administration, software engineering, and IT management. For the past 10 years he has been part-time teaching at colleges and doing corporate training. For the past 7 years, he has also been an independent consultant working with a variety of companies and serving as an expert consultant/witness in various computer cases. Chuck holds more than 28 different IT industry certifications, including the CISSP, ISSAP, Certified Ethical Hacker, Certified Hacking Forensics Investigator, EC Council Certified Security Administrator, and EC Council Certified Instructor. He has served as a subject matter expert for the Computer Technology Industry Association (CompTIA) in the development or revision of four of their certification tests, including the initial creation of their Security+ certification. Most recently he worked with the EC Council to develop their new advanced cryptography course, which he is teaching around the world.

In addition to this book, Chuck has authored 12 other titles on topics such as computer security, web development, programming, Linux, and computer crime. Chuck also is a frequent guest speaker for computer groups, discussing computer security. You can reach Chuck at his website www.chuckeasttom.com or by email at chuck@chuckeasttom.com

About the Technical Reviewer

Dr. Louay Karadsheh has a Doctorate of Management in information technology from Lawrence Technological University, Southfield, MI. He teaches information assurance, operating system, and networking classes. His research interest includes cloud computing, information assurance, knowledge management, and risk management. Dr. Karadsheh has published nine articles in refereed journals and international conference proceedings. He has 21 years of experience in planning, installation, troubleshooting, and designing local area networks and operating systems for small to medium-size sites. Dr. Karadsheh has provided technical edits/reviews for several major publishing companies, including Pearson Education and Cengage Learning, and evaluates the research proposals. He holds A+ and Security Certified Network professional certifications.

Dedication

This book is dedicated to my son AJ, who has been wonderful and supportive in all of my books.

Acknowledgments

The creation of a book is not a simple process and requires the talents and dedication from many people to make it happen. With this in mind, I would like to thank the folks at Pearson for their commitment to this project.

Specifically, I would like to say thanks to Betsy Brown for overseeing the project and keeping things moving. A special thanks to Dayna Isley for outstanding editing and focus. Also, thanks to Dr. Karadsheh, who worked tirelessly technically editing this book and fact checking it.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As an associate publisher for Pearson, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: David Dusthimer
Associate Publisher
Pearson Certification
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

It has been more than 6 years since the publication of the original edition of this book. A great deal has happened in the world of computer security since that time. This edition is updated to include newer information, updated issues, and revised content.

The real question is who is this book for. This book is a guide for any computer-savvy person. That means system administrators who are not security experts or anyone who has a working knowledge of computers and wishes to know more about cyber crime and terrorism could find this book useful. However, the core audience will be students who wish to take a first course in security but may not have a thorough background in computer networks. The book is in textbook format, making it ideal for introductory computer security courses that have no specific prerequisites. That lack of prerequisites means that people outside the normal computer science and computer information systems departments could also avail themselves of a course based on this book. This might be of particular interest to law enforcement officers, criminal justice majors, and even business majors with an interest in computer security.

As was previously mentioned, this book is intended as an introductory computer security book. In addition to the numerous end notes, the appendices will guide you to a plethora of additional resources. There are also review questions and practice exercises with every chapter.

This book is not a cookbook for hackers. You will see exactly how hackers target a system and get information about it. You will also see step-by-step instructions on how to use some password cracking utilities and some network scanning utilities. You will also be given a reasonably in depth explanation of various hacking attacks. However, you won't see a specific step-by-step recipe for executing an attack.

This book assumes that you are a competent computer user. That means you have used a computer at work and at home, are comfortable with email and web browsers, and know what words like *RAM* and *USB* mean. For instructors considering this as a textbook, that means that students will have had some basic understanding of PCs, but need not have had formal computer courses. For this reason, there is a chapter on basic networking concepts to get you up to speed. For readers with more knowledge, such as system administrators, you will find some chapters of more use to you than others. Feel free to simply skim any chapter that you feel is too elementary for you.

Chapter 3

Cyber Stalking, Fraud, and Abuse

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Know the various types of Internet investment scams and auction frauds
- Know specific steps one can take to avoid fraud on the Internet
- Have an understanding of what identity theft is and how it is done
- Know specific steps that can be taken to avoid identity theft
- Understand what cyber stalking is, and be familiar with relevant laws
- Know how to configure a web browser's privacy settings
- Know what laws apply to these computer crimes

Introduction

In every new frontier, a criminal element is bound to emerge. In times past, the high seas gave rise to pirates, and America's wild west produced gangs of outlaws. The Internet is no different than any other frontier; it has its share of outlaws. Besides hacking and virus creation, both mentioned in Chapter 1, "Introduction to Computer Security," there are other dangers. Fraud is one of the most common dangers of the Internet. As more people utilize the Internet as a conduit for commerce, there arises a greater opportunity for fraud. Fraud has been a part of life for as long as civilization has existed; in past centuries "snake oil" salesmen roamed the country selling face cures and elixirs. The Internet makes such fraud even easier. In fact, many experts would consider fraud to be the most prevalent danger on the Internet. There are multiple reasons for the popularity of Internet fraud among con artists. First, committing an Internet fraud does not require the technical expertise that hacking and virus creation require. Second, there are a great number of people engaging in various forms of online commerce, and this large amount of business creates a great many opportunities for fraud.

There are many avenues for fraud on the Internet. In this chapter, we will explore what the various major types of fraud are, what the law says, and what you can do to protect yourself. Fortunately for some readers, this particular chapter is not particularly technical, because most Internet fraud does not rely on in-depth technological expertise. Internet fraud merely uses the computer as a venue for many of the same fraud schemes that have been perpetrated throughout history.

How Internet Fraud Works

There are a variety of ways that a fraud can be perpetrated via the Internet. The Securities and Exchange Commission lists several types of Internet fraud on their website;[1] we will briefly discuss each of those and others, but it is not possible for us to cover every variation of each fraud scheme that has been used on the Internet. Such an undertaking would not only fill an entire book, but also possibly several volumes. What we can do is to cover the more common scams, and try to extrapolate some general principles that you can apply to any potential fraud. If you use these specific cases to extrapolate some general principles, then you should be prepared to avoid most fraud schemes.

Investment Offers

Investment offers are nothing new. Even some legitimate stockbrokers make their living by cold calling, the process of simply calling people (perhaps from the phone book), and trying to get them to invest in a specific stock. This practice is employed by some legitimate firms, but it is also a favorite con game for perpetrators of fraud. The Internet has allowed investment offers—both genuine and fraudulent—to be more easily disseminated to the general public. Most readers are probably familiar with investment offers flooding their inbox on a daily basis. Some of these email notifications entice you to become directly involved with a particular investment plan; other emails offer seemingly unbiased information from investors, free of charge. (Unfortunately, much of this advice is not as unbiased as it might appear to be.) While legitimate online newsletters can help investors gather valuable information, keep in mind that some online newsletters are fraudulent.

Common Schemes

One of the more common schemes involves sending out an email that suggests that you can make an outrageous sum of money with a very minimal investment. Perhaps the most famous of these schemes has been the Nigerian fraud. In this scenario, an email is sent to a number of random email addresses. Each one contains a message purporting to be from a relative of some deceased Nigerian doctor or government official. The deceased person will be someone you would associate with significant social standing, thus increasing the likelihood that you would view the offer more favorably. The offer goes like this: A person has a sum of money he wishes to transfer out of his country, and for security reasons, he cannot use normal channels. He wishes to use your bank account to “park” the funds temporarily. If you will allow him access to your account, you will receive a hefty fee. If you do agree to this arrangement, you will receive, via normal mail, a variety of very official-looking documents, enough to convince most casual observers that the arrangement is legitimate. You will then be asked to

advance some money to cover items such as taxes and wire fees. Should you actually send any money, you will have lost the money you advanced and you will never hear from these individuals again. The U.S. Secret Service has a bulletin issued detailing this particular fraud scheme.[2]

Now consider this investment scam, and variations of it, from a logical point of view. If you had large sums of money you needed to transfer, would you send it to a person in a foreign country, someone you had never met? Wouldn't you be worried that the recipient would cash out her account and take the next plane to Rio? If a person needs to transfer money internationally, why doesn't he just transfer the money to an account in the Bahamas? Or cash out the account and send it via Federal Express or United Parcel Service to a storage facility in the United States? The point is that there are many ways a person could get money out of a country without trusting some stranger he has never seen before. That fact alone should indicate to you that this offer is simply not legitimate. This concept is the first general principle you should derive concerning fraud. In any offer, consider the point of view of the person offering it. Does it sound as if he is taking an inordinately large risk? Does the deal seem oddly biased in your favor? Put yourself in his position. Would you engage in the deal if you where in his position? If not, then this factor is a sign that the deal might not be what it seems.

Investment Advice

Such blatant fraud schemes are not the only investment pitfall on the Internet. Some companies pay the people who write online newsletters to recommend their stocks. While this activity isn't actually illegal, U.S. federal securities laws do require the newsletters to disclose that they where paid to proffer this advice. Such laws are in place because when the writers are recommending any product, their opinion might be swayed by the fact that compensation is being provided to them for that opinion. Many online investment newsletters do not disclose that they are actually being paid to recommend certain stocks. This situation means that the "unbiased" stock advice you are getting could actually be quite biased. Rather than getting the advice of an unbiased expert, you may be getting a paid advertisement. This pitfall is one of the most common traps of online investment advice, more common than the blatant frauds.

Sometimes these online stock bulletins can be part of a wider scheme, often called a pump and dump. A classic pump and dump is rather simple. The con artist takes a stock that is virtually worthless and purchases large amounts of the stock. The con artist then artificially inflates the value,[3] in several ways. One common method is to begin circulating rumors on various Internet bulletin boards and chat rooms that the stock is about to go up significantly. Often it is suggested by the trickster that the company has some new innovative product due to come out in the next few weeks. Another method is to simply push the stock on as many people as possible. The more people vying to buy a stock, the higher its price will rise. If both methods are combined, it is possible to take a worthless stock and temporarily double or triple its value. The perpetrator of the fraud has already purchased volumes of the stock, at a very low price, before executing this scheme. When the stock goes as high as she thinks it can, she then dumps her stock and takes the money. In a short time, and certainly by the time the company's next quarterly earnings report is released, the stock returns to its real value. This sort of scheme has been very popular in the past several decades; thus, you should always be wary of such "insider" information. If a person

is aware that Company X is about to release an innovative new product that will drive her stock value up, why would she share that information with total strangers?

The U.S. Securities and Exchange Commission lists several tips for avoiding such scams:[4]

1. Consider the source. Especially if you are not well versed in the market, make sure you accept advice only from well-known and reputable stock analysts.
2. Independently verify claims. Do not simply accept someone else's word about anything.
3. Research. Read up on the company, the claims about the company, its stock history, and so forth.
4. Beware of high-pressure tactics. Legitimate stock traders do not pressure customers into buying. They help customers pick stocks that customers want. If you are being pressured, that is an indication of potential problems.
5. Be skeptical. A healthy dose of skepticism can save you a lot of money. Or, as the saying goes, "If it's too good to be true, it probably isn't."
6. Make sure you thoroughly research any investment opportunity.

The truth is that these types of fraud depend on the greed of the victim. It is not my intent to blame victims of fraud, but it is important to realize that if you allow avarice to do your thinking for you, you are a prime candidate to be a victim of fraud. Your 401K or IRA may not earn you exorbitant wealth overnight, but they are steady and relatively safe. (No investment is completely safe.) If you are seeking ways to make large sums of money with minimal time and effort, then you are an ideal target for perpetrators of fraud.

In Practice

Practically speaking, the recommended way to handle online investments is to only participate in them if you initiated the discussion with a reputable broker. This would mean you would never respond to or participate in any investment offer that was sent to you via email, online ads etc. You would only participate in investments that you initiated with well-known brokers. Usually such brokers are traditional investment firms with long-standing reputations that now simply offer their services online. It is also important to check out any broker with the Securities and Exchange Commission (SEC).

Auction Frauds

Online auctions, such as eBay, can be a wonderful way to find merchandise at very good prices. I routinely use such auctions to purchase goods. However, any auction site can be fraught with peril. Will you actually get the merchandise you ordered? Will it be "as advertised"? Most online auctions

are legitimate, and most auction websites take precautions to limit fraud on their website. But problems still occur. In fact, the U.S. Federal Trade Commission[5] (FTC) lists the following four categories of online auction fraud:

- Failure to send the merchandise
- Sending something of lesser value than advertised
- Failure to deliver in a timely manner
- Failure to disclose all relevant information about a product or terms of the sale

The first category, failure to deliver the merchandise, is the most clear-cut case of fraud and is fairly simple. Once you have paid for an item, no item arrives. The seller simply keeps your money. In organized fraud, the seller will simultaneously advertise several items for sale, collect money on all the auctions, and then disappear. If he or she has planned this well, the entire process was done with a fake identification, using a rented mailbox and anonymous email service. The person then walks away with the proceeds of the scam.

The second category of fraud, delivering an item of lesser value than the one advertised, can become a gray area. In some cases, it is outright fraud. The seller advertises something about the product that simply is not true. For example, the seller might advertise a signed copy of the first printing of a famous author's book, but then instead ship you a fourth printing with either no autograph, or one that is unverified. However, in other cases of this type of problem, it can simply be that the seller is overzealous, or frankly mistaken. The seller might claim his baseball was signed by a famous athlete, but not be aware himself that the autograph is a fraud.

This problem is closely related to the fourth item on the FTC list, failure to disclose all relevant facts about the item. For example, a book might be an authentic first printing and autographed, but be in such poor physical condition as to render it worthless. This fact may or may not be mentioned in advance by the seller. Failure to be forthcoming with all the relevant facts about a particular item might be the result of outright fraud or simply of the seller's ignorance. The FTC also lists failure to deliver the product on time as a form of fraud. It is unclear whether or not that is fraud in many cases, or merely woefully inadequate customer service.

The Federal Trade Commission and Auction Fraud

The FTC also lists three other areas of bidding fraud that are growing in popularity on the Internet. From the FTC website:[5]

- *Shill bidding,* when fraudulent sellers (or their "shills") bid on the seller's items to drive up the price.
- *Bid shielding,* when fraudulent buyers submit very high bids to discourage other bidders from competing for the same item. The fake buyers then retract their bids so that people they know can get the item at a lower price.

- *Bid siphoning*, when con artists lure bidders off legitimate auction sites by offering to sell the "same" item at a lower price. Their intent is to trick consumers into sending money without proffering the item. By going off-site, buyers lose any protections the original site may provide, such as insurance, feedback forms, or guarantees.

Shill Bidding

Shill bidding has been probably the most common of these three auction frauds. It is not very complex. If the perpetrator is selling an item at an auction site, she will also create several fake identities. She will use these fake identities to bid on the item and thus drive the price up. It is very difficult to detect if such a scheme is in operation. However, a simple rule of thumb on auctions is to decide, before you start bidding, what your maximum price is. And then, under no circumstances, do you exceed that price, by even one penny.

Bid Shielding

While shill bidding may be difficult to combat, bid shielding can be addressed fairly easily by the proprietors of the auction site. Many of the major auction sites, such as eBay, have taken steps to prevent bid shielding. The most obvious is to revoke bidding privileges for bidders who back out after they have won an auction. So if a person puts in a very high bid to keep others away, then at the last moment retracts his bid, he might lose his ability to be on that auction site.

Bid Siphoning

Bid siphoning is a less-common practice. In this scheme, the perpetrator places a legitimate item up for bid on an auction site. But then, in the ad for that item, she provides links to sites that are not part of the auction site. The unwary buyer who follows those links might find himself on an alternative site that is a "setup" to perpetrate some sort of fraud.

All of these tactics have a common aim: to subvert the normal auction process. The normal auction process is an ideal blend of capitalism and democracy. Everyone has an equal chance to obtain the product in question, if he or she is willing to outbid the other shoppers. The buyers themselves set the price of the product, based on the value they perceive the product to have. In my opinion, auctions are an excellent vehicle for commerce. However, unscrupulous individuals will always attempt to subvert any process for their own goals.

Identity Theft

Identity theft is a growing problem and a very troubling one. The concept is rather simple, though the process can be complex, and the consequences for the victim can be quite severe. The idea is simply for one person to take on the identity of another. This is usually attempted to make purchases; but identity theft can be done for other reasons, such as obtaining credit cards in the victim's name, or even driver's

licenses. If the perpetrator obtains a credit card in someone else's name, then he can purchase products and the victim of this fraud is left with debts she was not aware of and did not authorize.

In the case of getting a driver's license in the victim's name, this fraud might be attempted to shield the perpetrator from the consequences of his or her own poor driving record. For example, a person might get your driving information to create a license with his or her own picture. Perhaps the criminal in this case has a very bad driving record and even warrants out for immediate arrest. Should the person be stopped by law enforcement officers, he or she can then show the fake license. When the police officer checks the license, it is legitimate and has no outstanding warrants. However, the ticket the criminal receives will be going on your driving record, because it is your information on the driver's license. It is also unlikely that the perpetrator of that fraud will actually pay the ticket, so at some point you—whose identity was stolen—will receive notification that your license has been revoked for failure to pay a ticket. Unless you can then prove, with witnesses, that you were not at the location the ticket was given at the time it was given, you may have no recourse but to pay the ticket, in order to reestablish your driving privileges.

The U.S. Department of Justice defines identity theft in this manner:[6]

> "*Identity theft* and *identity fraud* are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."

The advent of the Internet has made the process of stealing a person's identity even easier than it used to be. Many states now have court records and motor vehicle records online. In some states, a person's social security number is used for the driver's license number. So if a criminal gets a person's social security number, he or she can look up that person's driving record, perhaps get a duplicate of the person's license, find out about any court records concerning that person, and on some websites, even run the person's credit history. Later in this book, we will examine using the Internet as an investigative tool. Like any tool, it can be used for benign or malevolent purposes. The same tools you can use to do a background check on a prospective employee can be used to find out enough information to forge someone else's identity.

FYI: Alternate Means of Identity Theft

There are other means for a perpetrator to conduct identity theft that do not involve the Internet. A ring of criminals in the Dallas-Fort Worth metroplex were working with waiters in restaurants. When the waiter took your credit card or debit card to pay for the meal, they would also use a small hand held device (kept hidden in a pocket) to scan in your credit card information. They would then give this information to the identity theft ring, who could either make online purchases or use that information to produce fake credit cards with your name and account data. This is a new twist on identity theft. The only way to avoid this sort of danger is to never use your credit or debit card unless it is going to be processed right there in front of you. Do not let someone take your card out of your site to process it.

Phishing

One of the more common ways to accomplish identity theft is via a technique called phishing, which is the process of trying to induce the target to provide you with personal information. For example the attacker might send out an email purporting to be from a bank, and telling recipients that there is a problem with their bank account. The email then directs them to click on a link to the bank website where they can login and verify their account. However, the link really goes to a fake website set up by the attacker. When the target goes to that website and enters his information, he will have just given his username and password to the attacker.

Many end users today are aware of these sorts of tactics and avoid clicking on email links. But unfortunately, not everyone is so prudent, and this attack still is effective. It is also the case that the attackers have come up with new ways of phishing. One of these methods is called cross-site scripting. If a website allows users to post content that other users can see (such as a product review) the attacker then posts, but instead of posting a review or other legitimate content, they post a script (i.e., JavaScript or something similar). Now when other users visit that web page, instead of loading a review or comment, it will load the attacker's script. That script may do any number of things, but it is common for the script to redirect the end user to a phishing website. If the attacker is clever, the phishing website looks identical to the real one, and end users are not aware they have been redirected. Cross-site scripting can be prevented by web developers filtering all user input.

Cyber Stalking

Stalking in general has received a great deal of attention in the past few years. The primary reason is that stalking has often been a prelude to violent acts, including sexual assault and homicide. For this reason, many states have passed a variety of antistalking laws. However, stalking has expanded into cyberspace. What is cyber stalking? It is using the Internet to harass another person; or, as the U.S. Department of Justice[7] puts it:

> "Although there is no universally accepted definition of *cyber stalking*, the term is used in this report to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family; and still others require only that the alleged stalker's course of conduct constitute an implied threat. While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously."

If someone uses the Internet to harass, threaten, or intimidate another person, then the perpetrator is guilty of cyber stalking. The most obvious example is sending threatening email. The guidelines on what is considered "threatening" can vary a great deal from jurisdiction to jurisdiction. But a good rule

of thumb is that if the email's content would be considered threatening in normal speech, then it will probably be considered a threat if sent electronically. Other examples of cyber stalking are less clear. If you request that someone quit emailing you, yet they continue to do so, is that a crime? Unfortunately, there is no clear answer on that issue. The truth is that it may or may not be considered a crime, depending on such factors as the content of the emails, the frequency, the prior relationship between you and the sender, as well as your jurisdiction.

Real Cyber Stalking Cases

The following three cases, also from the Department of Justice website,[7] illustrate cases of cyber stalking. Examining the facts in these cases might help you to get an idea of what legally constitutes cyber stalking.

1. In the first successful prosecution under California's new cyber stalking law, prosecutors in the Los Angeles District Attorney's Office obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. The former security guard pleaded guilty in April 1999 to one count of stalking and three counts of solicitation of sexual assault. He faces up to six years in prison.
2. A local prosecutor's office in Massachusetts charged a man who, using anonymous re-mailers, allegedly engaged in a systematic pattern of harassment of a co-worker, which culminated in an attempt to extort sexual favors from the victim under threat of disclosing past sexual activities to the victim's new husband.
3. An honors graduate from the University of San Diego terrorized five female university students over the Internet for more than a year. The victims received hundreds of violent and threatening emails, sometimes receiving four or five messages a day. The graduate student, who has entered a guilty plea and faces up to six years in prison, told police he committed the crimes because he thought the women were laughing at him and causing others to ridicule him. In fact, the victims had never met him.

Clearly, using the Internet to harass people is just as serious a crime as harassing them in person. This problem has even extended to workplace issues. For example, court cases have upheld that unwanted email pornography can be construed as sexual harassment. If an employee complains about unwanted email, the employer has a duty to at least attempt to ameliorate the situation. This attempt can be as simple as installing a very inexpensive spam blocker (software that tries to limit or eradicate unwanted email). However, if the employer takes no steps whatsoever to correct the problem, that reticence may be seen by a court as contributing to a hostile work environment. As previously stated, if the stalking act would constitute as harassment in person, then it would be considered harassment in cyberspace. *Black's Law Dictionary*[8] defines *harassment* as follows:

> "A course of conduct directed at a specific person that causes substantial emotional distress in such person and serves no legitimate purpose."
>
> "Words, gestures, and actions that tend to annoy, alarm, and abuse (verbally) another person."

Usually law enforcement officials will need some credible threat of harm in order to pursue harassment complaints. In simple terms, this situation means that if you are in an anonymous chat room and someone utters some obscenity, that act probably will not be considered harassment. However, if you receive specific threats via email, those threats would probably be considered harassment.

Laws about Internet Fraud

Over the past several years, various legislatures (in the United States and in other countries) have passed laws defining *Internet fraud* and stating the proscribed punishments. In many cases, existing laws against fraud and harassment are applicable to the Internet as well; however, some legislators have felt that cyber crime warranted its own distinct legislation.

Identity theft has been the subject of various state and federal laws. Most states now have laws against identity theft.[9] This crime is also covered by federal law. In 1998, the federal government passed 18 U.S.C. 1028, also known as The Identity Theft and Assumption Deterrence Act of 1998. This law made identity theft a federal crime.[10] Throughout the United States, federal law now covers identity theft, and in many states identity theft is also covered by state law.

Many states specifically prohibit cyber stalking; and in general, existing anti-stalking laws can be applied to the Internet. In 2001, in California a man was convicted of cyber stalking under existing antistalking statutes.[11] Other countries also have existing antistalking laws that can be applied to cyber stalking as well. Canada has had a comprehensive antistalking law since 1993. Unfortunately, there are many similar cases. Just a few include the following:

- From 2010, there is the case of Joseph Medico (70 years old), who met a 16-year-old girl at his church. Mr. Medico followed the girl to her car and tried to talk her into going to dinner with him and then back to his home. When she rejected his advances, he began calling and texting her several times a day. His activities escalated until the girl reported the activities and Mr. Medico was arrested for stalking.
- In 2008 Shawn Michael Hutchinson, 20, posted threats and nude pictures of a former girlfriend. His threats included statements such as '"I told you that if I saw you with David that would be the end of you. That's not a threat, it's a promise."

One nation that has decided to crack down hard on cyber criminals is Romania. Some experts have described Romanian cyber crime law as the strictest in the world.[12] However, what is most interesting about Romanian law is how specific it is. The crafters of this legislation went to some effort to very specifically define all the terms used in the legislation. This specificity is very important in order to avoid defendants finding loopholes in laws. Unfortunately, the Romanian government only took such measures after media sources around the world identified their country as a "Citadel for Cyber Crime." The country's reactive approach to cyber crime is probably not the best solution.

The University of Dayton School of Law has an entire website devoted to cyber crime.[13] The school has some rather extensive links on cyber crime, cyber stalking, and other Internet-based crimes. As we move forward in the twenty-first century, one can expect to see more law schools with courses dedicated to cyber crime.

An interesting phenomenon has begun in the past few years: the emergence of attorneys who specialize in cyber crime cases. The fact that there are lawyers who specialize in this area of law is a strong indicator that Internet crime is becoming a growing problem in modern society.

Protecting Yourself against Cyber Crime

Now that you know about the various frauds that are prevalent on the Internet and have looked at the relevant laws, you might be wondering what you can do to protect yourself. There are several specific steps you can take to minimize the chances of being the victim of Internet crime. There are also some clear guidelines on how you should handle the situation, should you become a victim.

Protecting against Investment Fraud

To protect yourself against investment fraud, follow these guidelines:

1. Only invest with well-known, reputable brokers.
2. If it sounds too good to be true, then avoid it.
3. Ask yourself why this person is informing you of this great investment deal. Why would a complete stranger decide to share some incredible investment opportunity with you?
4. Remember that even legitimate investment involves risk, so never invest money that you cannot afford to lose.

Protecting against Identity Theft

When the issue is identity theft, your steps are clear:

1. Do not provide your personal information to anyone if it is not absolutely necessary. This rule means that when communicating on the Internet with anyone you do not personally know, do not reveal anything about yourself; not your age, occupation, real name, nothing.
2. Destroy documents that have personal information on them. If you simply throw away bank statements and credit card bills, then someone rummaging through your trash can get a great deal of personal data. You can obtain a paper shredder from an office supply store or many retail department stores for less than $20. Shred these documents before disposing of them. This rule may not seem like it is related to computer security, but information gathered through nontechnical means can be used in conjunction with the Internet to perpetrate identity theft.

3. Check your credit frequently. Many websites, including www.consumerinfo.com, allow you to check your credit and even get your beacon score for a nominal fee. I check my credit twice per year. If you see any items you did not authorize, that is a clear indication that you might be a victim of identity theft.
4. If your state has online driving records, then check yours once per year. If you see driving infractions that you did not commit, this evidence is a clear sign that your identity is being used by someone else. In an upcoming chapter on cyber detective work, we will explore in detail how to obtain such records online, often for less than $5.

To summarize, the first step in preventing identity theft is restricting the amount of personal information you make available. The next step is simply monitoring your credit and driving records so that you will be aware if someone attempts to use your identity.

Another part of protecting your identity is protecting your privacy in general. That task means preventing others from gaining information about you that you don't explicitly provide them. That preventative method includes keeping websites from gathering information about you without your knowledge. Many websites store information about you and your visit to their site in small files called *cookies*. These cookie files are stored on your machine. The problem with cookies is that any website can read any cookie on your machine, even ones that the website you are currently visiting did not create. So if you visit one website and it stores items like your name, the site you visited, and the time you where there, then another website could potentially read that cookie and know where you have been on the Internet. One of the best ways to stop cookies you don't want is anti-spyware software. We will discuss such software in more detail in a later chapter. Right now, let's see how to change your Internet settings to help reduce exposures to your privacy.

Secure Browser Settings

If you are using Microsoft Internet Explorer, you can go to Tools and use the drop-down menu; then select Options. You will then see a screen much like the one shown in Figure 3.1. You can then select the third tab, labeled Privacy.

When you select that Privacy tab, you will see the screen shown in Figure 3.2. Notice the sliding bar on the left that lets you select various levels of general protection against cookies. It is recommended that you select Medium High as your level.

Note the Advanced button at the bottom of the screen. This button allows you to block or allow individual websites from creating cookies on your computer's hard drive. Altering cookie settings on your machine is just one part of protecting your privacy, but it is an important part.

You probably also want to ensure that you have selected the In Private browsing option, also shown in Figure 3.2.

If you are working with Firefox, the process is similar. You select Tools from the drop-down menu, then select Options. You will then see the screen shown in Figure 3.3.

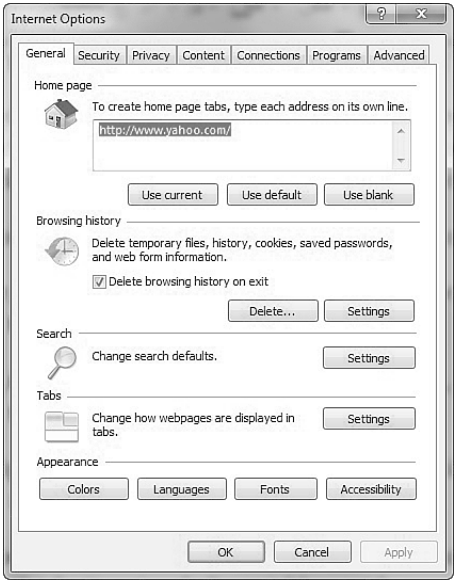

FIGURE 3.1 Internet Explorer options.

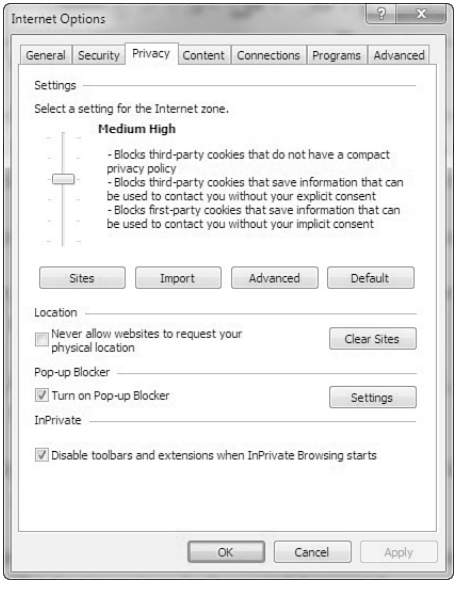

FIGURE 3.2 Internet Explorer privacy options.

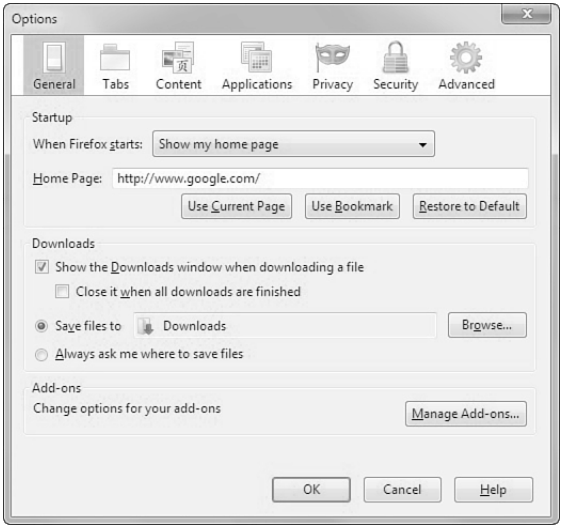

FIGURE 3.3 Firefox options.

Notice the Privacy option and you will see a screen much like the one shown in Figure 3.4.

FIGURE 3.4 Firefox privacy.

As you can see from Figure 3.4, there are a number of privacy settings for you to select, and they are self-explanatory. You can also select the Security tab and see the screen in Figure 3.5.

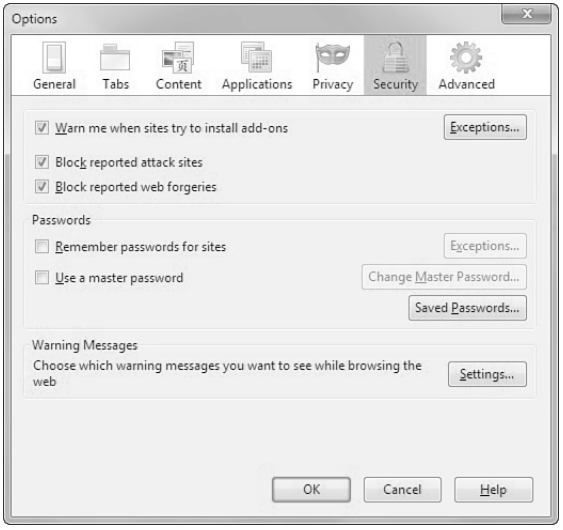

FIGURE 3.5 Firefox security.

I recommend selecting High Security. Also, I would only allow first-party cookies. Third-party cookies are notorious for behaving in ways that violate user privacy. We will discuss cookies and spyware in much more detail in a later chapter, but the simple steps just examined can go a long way toward helping to secure your privacy.

Dealing with auction fraud involves a different set of precautions; here are four good ideas.

1. Only use reputable auction sites. The most well-known site is eBay, but any widely known, reputable site will be a safer gamble. Such auction sites tend to take precautions to prevent fraud and abuse.
2. If it sounds too good to be true, don't bid.
3. Some sites actually allow you to read feedback other buyers have provided on a given seller. Read the feedback, and only work with reputable sellers.
4. When possible use a separate credit card, one with a low limit, for online auctions. That way, should your credit card be compromised, your liability is limited. Using your debit card is simply inviting trouble.

Online auctions can be a very good way to get valuable merchandise at low prices. However one must exercise some degree of caution when using these services.

Protecting yourself from online harassment also has its own guidelines:

1. If you use chat rooms, discussion boards, and so forth, do not use your real name. Set up a separate email account with an anonymous service, such as Yahoo!, Gmail, or Hotmail. Then use that account and a fake name online. This makes it very hard for an online stalker to trace back to you personally.
2. If you are the victim of online harassment, keep all the emails in both digital and printed format. Use some the investigative techniques we will explore later in this book to try and identify the perpetrator. If you are successful, then you can take the emails and the information on the perpetrator to law enforcement officials.
3. Do not, in any case, ignore cyber stalking. According to the Working to Halt Online Abuse website,[14] 19% of cyber stalking cases escalate to stalking in the real world.

It is not the intent of this chapter or of this book to make you frightened about using the Internet. My family routinely uses the Internet for entertainment, commerce, and informational purposes. One simply needs to exercise some caution when using the Internet.

Summary

Clearly, fraud and identity theft are very real and growing problems. In our modern age of instant access to information and online purchasing, it is critical that every person take steps to protect themselves against this issue. Individuals must work to protect their privacy, using steps outlined in this chapter. It is also imperative for law enforcement officers to obtain the skills needed to investigate and solve these sorts of cyber crimes.

Cyber stalking is one area that is often new to both civilians and law enforcement. It is very important that both groups have a clear understanding of what is, and is not, cyber stalking. Unfortunately, cyber stalking cases can escalate into real-world violence.

Test Your Skills

MULTIPLE CHOICE

1. The most common Internet investment fraud is known as what?
   - **A.** The Nigerian fraud
   - **B.** The Manhattan fraud
   - **C.** The pump and dump
   - **D.** The bait and switch
2. What is the most likely problem with unsolicited investment advice?
   - **A.** You might not earn as much as claimed.
   - **B.** The advice might not be truly unbiased.
   - **C.** The advice might not be from a legitimate firm.
   - **D.** You might lose money.
3. Artificially inflating a stock in order to sell it at a higher value is referred to as what?
   - **A.** Bait and switch
   - **B.** The Nigerian fraud
   - **C.** Pump and dump
   - **D.** The Wall Street fraud
4. What is the top rule for avoiding Internet fraud?
   - **A.** If it seems too good to be true, it probably is.
   - **B.** Never use your bank account numbers.
   - **C.** Only work with people who have verifiable email addresses.
   - **D.** Don’t invest in foreign deals.

5. Which of the following is not one of the Security and Exchange Commission's tips for avoiding investment fraud?

   A. Don't invest online.
   B. Consider the source of the offer.
   C. Always be skeptical.
   D. Always research the investment.

6. What are the four categories of auction fraud?

   A. Failure to send, failure to disclose, sending to wrong address, failure to deliver
   B. Failure to send, failure to disclose, sending something of lesser value, failure to deliver
   C. Failure to disclose, sending something to wrong address, failure to send, failure to deliver
   D. Failure to disclose, sending something of lesser value, failure to send, sending something of greater value

7. A seller bidding on his or her own item to drive up the price is referred to as what?

   A. Bid siphoning
   B. Bid shielding
   C. Shill bidding
   D. Ghost bidding

8. Submitting a fake but very high bid to deter other bidders is referred to as what?

   A. Bid siphoning
   B. Bid shielding
   C. Shill bidding
   D. Ghost bidding

9. Identity theft is most often attempted in order to accomplish what goal?

   A. To make illicit purchases
   B. To discredit the victim
   C. To avoid criminal prosecution
   D. To invade privacy

10. According to the U.S. Department of Justice, identity theft is generally motivated by what?

   A. Malicious intent
   B. Personal hostility towards the victim
   C. Economic gain
   D. Thrill seeking

11. Why is cyber stalking a serious crime?

- **A.** It is frightening to the victim.
- **B.** It can be a prelude to violent crime.
- **C.** It is using interstate communication.
- **D.** It can be a prelude to identity theft.

12. What is cyber stalking?

- **A.** Any use of the Internet to send or post threats
- **B.** Any use of electronic communications to stalk a person
- **C.** Only use of email to send threats
- **D.** Only the use of email to stalk a person

13. What will law enforcement officials usually require of the victim in order to pursue harassment allegations?

- **A.** A verifiable threat of death or serious injury
- **B.** A credible threat of death or serious injury
- **C.** A verifiable threat of harm
- **D.** A credible threat of harm

14. If you are posting anonymously in a chat room and another anonymous poster threatens you with assault or even death, is this person's post harassment?

- **A.** Yes, any threat of violence is harassment.
- **B.** Probably not, because both parties are anonymous, so the threat is not credible.
- **C.** Yes, chat room threats are no different than threats in person.
- **D.** Probably not, because making a chat room threat is not the same as making a threat in person.

15. What must exist for cyber stalking to be illegal in a state or territory?

- **A.** Specific laws against cyber stalking in that state or territory.
- **B.** Specific laws against cyber stalking in that nation.
- **C.** Nothing; existing stalking laws can apply.
- **D.** Nothing; existing international cyber stalking laws apply.

16. What is the first step in protecting yourself from identity theft?

    A. Never provide any personal data about yourself unless absolutely necessary.
    B. Routinely check your records for signs of identity theft.
    C. Never use your real name on the Internet.
    D. Routinely check for spyware on your computer.

17. What can you do on your local computer to protect your privacy?

    A. Install a virus scanner.
    B. Install a firewall.
    C. Set your browser's security settings.
    D. Set your computer's filter settings.

18. What is a cookie?

    A. A piece of data that web servers gather about you.
    B. A small file made that contains data and then is stored on your computer.
    C. A piece of data that your web browser gathers about you.
    D. A small file made that contains data and then is stored on the web server.

19. Which of the following is not an efficient method of protecting yourself from auction fraud?

    A. Only use auctions for inexpensive items.
    B. Only use reputable auction sites.
    C. Only work with well-rated sellers.
    D. Only bid on items that seem realistic.

20. The top rule for chat room safety is what?

    A. Make certain you have antivirus software installed.
    B. Never use your real name or any real personally identifying characteristics.
    C. Only use chat rooms that encrypt transmissions.
    D. Use chat rooms that are sponsored by well-known websites or companies.

21. Why is it useful to have a separate credit card dedicated to online purchases?

    A. If the credit card number is used illegally, you will limit your financial liability.
    B. You can keep better track of your auction activities.
    C. If you are defrauded, you can possibly get the credit card company to handle the problem.
    D. You can easily cancel that single card, if you need to do so.

22. What percentage of cyber stalking cases escalate to real-world violence?

    A. Less than 1%
    B. 25%
    C. 90% or more
    D. About 19%

23. If you are a victim of cyber stalking, what should you do to assist the police?

    A. Nothing; it is their job and you should stay out of it.
    B. Attempt to lure the stalker into a public place.
    C. Keep electronic and hard copies of all harassing communications.
    D. Try to provoke the stalker into revealing personal information about himself or herself.

24. What is the top way to protect yourself from cyber stalking?

    A. Do not use your real identity online.
    B. Always use a firewall.
    C. Always use a virus scanner.
    D. Do not give out email addresses.

EXERCISES

EXERCISE 3.1: Setting Web Browser Privacy in Internet Explorer

1. This process was described in detail with images in the chapter, but we will walk through the process here:
   - Select Tools from the drop-down menu at the top of Internet Explorer, then choose Internet Options.
   - Select the third tab, which is labeled Privacy.
   - Click the Advanced button.
   - Set your browser to accept first party cookies, prompt for third-party cookies, and accept session cookies.

EXERCISE 3.2: Using Alternative Web Browsers

1. Download the Firefox browser from www.mozilla.org.
2. Set privacy and security settings.

EXERCISE 3.3: Tracking in a Chat Room

The purpose of this exercise is to grasp how easy it is to obtain personal information about someone from his or her online activities.

1. Enter any chat room. If you are not familiar with chat rooms or have not used them before, any of the following websites would make a good starting point for you:

   http://chat.icq.com/icqchat/

   www.aol.com/community/chat/allchats.html

   www.javachatrooms.net/

   www.chat-avenue.com/

2. Note those people who use their real names.
3. Note those people who reveal personal details.
4. Compile as much information as you can about posers in the chat room.

CAUTION

The purpose of this exercise is merely to show you how easy it is for someone to learn about another person from his or her online activities. In no case would you consider using this information to invade another person's privacy or to harass or embarrass another person.

PROJECTS

PROJECT 3.1: Finding Out about Cyber Stalking and the Law

1. Using the Web or other resources, find out what your state, country, or province's laws are regarding cyber stalking.
2. Write a brief paper describing those laws and what they mean. You may select to do a quick summary of several laws or a more in-depth examination of one law. If you choose the former, then simply list the laws and write a brief paragraph explaining what they cover. If you choose the latter option, then discuss the law's authors, why it was written, and possible ramifications of the law.

PROJECT 3.2: Looking for Auction Fraud

Go to any auction site and try to identify if there are any sellers you feel might be fraudulent. Write a brief paper explaining what about that seller indicated that he or she may not be dealing honestly.

PROJECT 3.3: Examining Cyber Stalking Case Studies

1. Using the Web, find a case of cyber stalking not mentioned in this chapter. You may find some of the following websites helpful:

   www.safetyed.org/help/stalking/

   www.cyber-stalking.net/

   www.technomom.com/harassed/index.shtml

2. Write a brief paper discussing this case, with particular attention to steps you think might have helped avoid or ameliorate the situation.

Case Study

Consider the case of an intrepid identity thief. The perpetrator, Jane, encounters the victim, John, online in a chat room. John is using his real first name, but only his last initial. However, over a series of online conversations between Jane and John, he does reveal personal details about his life (marital status, children, occupation, region he lives in, and so forth). Eventually, Jane offers John some piece of information, such as perhaps an investment tip, as a trick to get John's email address from him. Once she gets his email address, an email exchange begins outside of the chat room, wherein Jane purports to give John her real name, thus encouraging John to do the same. Of course, the perpetrator's name is fictitious, such as "Mary." But Jane now has John's real name, city, marital status, occupation, and so on.

Jane has a number of options she can try, but we will choose a simple one. She begins by using the phone book or the Web to get John's home address and phone number. She can then use this information to get John's social security number, in a variety of ways. The most straightforward would be to go through John's trash while he is at work. However, if John works in a large company, Jane can just call (or enlist someone to call), claiming to be John's wife or another close relative, wanting to verify personnel data. If Jane is clever enough, she may come away with John's social security number. Then it is a trivial matter (as we will see in Chapter 13, "Cyber Detective") to get John's credit report and to get credit cards in his name.

From this scenario, consider the following questions:

1. What reasonable steps could John have taken to protect his identity in the chat room?
2. What steps should any employer take to prevent being unwittingly complicit in identity theft?

Chapter Footnotes

1. The U.S. Securities and Exchange Commission. "Internet Fraud: How to Avoid Internet Investment Scams." Washington, D.C.: Author, November 15, 2001. Accessed April 2011: www.sec.gov/investor/pubs/cyberfraud.htm

2. The U.S. Secret Service. "Public Awareness Advisory Regarding '4-1-9' or 'Advance Fee Fraud' Schemes." Washington, D.C.: Author, 2002. Accessed April 2011: http://www.lbl.gov/IT/CIS/CITG/email/419-Fraud.html

3. The Fraud Bureau. "Pump and Dump Classic." Stock Scams 101. Ontario: Fraud Bureau Corporation, 1999. Accessed April 2011: www.fraudbureau.com/investor/101/article15.html

4. The U.S. Securities and Exchange Commission "Pump+Dump.con: Avoiding Stock Scams on the Internet." Washington, D.C.: Author, September 8, 2000. April 2011: www.sec.gov/investor/pubs/pump.htm

5. The U.S. Federal Trade Commission, Accessed April 2011: www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt124.shtm

6. The U.S. Department of Justice Identity Theft web page, Accessed April 2011: www.justice.gov/criminal/fraud/websites/idtheft.html

7. The U.S. Department of Justice Cyber Stalking page. Accessed April 2011: www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

8. *Blacks Law Dictionary*, 1999, West Publishing Company, 7th Edition.

9. The National Conference of State Legislatures. "State Computer Harassment or 'Cyberstalking' Laws." Denver and Washington, DC.: Author, 2004. Accessed April 2011: www.ncsl.org/programs/lis/cip/stalk99.htm

10. The Identity Theft and Deterrence Act of 1998, USC 1028

11. *The Minneapolis-St.Paul Star Tribune*, Accessed August 23, 2001: www.startribune.com/

12. Romanian Information Technology Initiative. Accessed April 2011: www.riti-internews.ro/cybercrime.htm

13. University of Dayton School of Law. Accessed November 2003: cybercrimes.net/

14. Working to Halt Online Abuse. Accessed April 2011: www.haltabuse.org/

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q–R

S

T

U

V

W

X–Z