



COMPUTER SECURITY FUNDAMENTALS

SECOND EDITION

CHUCK EASTTOM

Computer Security Fundamentals

Chuck Easttom

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Computer Security Fundamentals

Copyright © 2012 by Pearson

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

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

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

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Que Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Bulk Sales

Que Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales

1-800-382-3419

corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales

international@pearson.com

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

	Introduction	1
1	Introduction to Computer Security	2
2	Networks and the Internet	22
3	Cyber Stalking, Fraud, and Abuse	48
4	Denial of Service Attacks	72
5	Malware	92
6	Techniques Used by Hackers	116
7	Industrial Espionage in Cyberspace	132
8	Encryption	154
9	Computer Security Software	178
10	Security Policies	200
11	Network Scanning and Vulnerability Scanning	220
12	Cyber Terrorism and Information Warfare	254
13	Cyber Detective	276
14	Introduction to Forensics	292
A	Glossary	306
B	Resources	312
	Index	316

Table of Contents

Introduction	1
Chapter 1: Introduction to Computer Security	2
Introduction	2
How Seriously Should You Take Threats to Network Security?	3
Identifying Types of Threats	4
Malware	5
Compromising System Security	6
Denial of Service Attacks	7
Web Attacks	7
Session Hijacking	7
DNS Poisoning	7
Assessing the Likelihood of an Attack on Your Network	7
Basic Security Terminology	8
Hacker Slang	8
Professional Terms	10
Concepts and Approaches	11
How Do Legal Issues Impact Network Security?	13
Online Security Resources	14
CERT	14
Microsoft Security Advisor	14
F-Secure	14
SANS Institute	14
Summary	15
Test Your Skills	15
Chapter 2: Networks and the Internet	22
Introduction	22
Network Basics	23

The Physical Connection: Local Networks	23
Faster Connection Speeds	26
Data Transmission	26
How the Internet Works	28
IP Addresses	28
CIDR	31
Uniform Resource Locators	32
History of the Internet	33
Basic Network Utilities	35
IPConfig	35
Ping	36
Tracert	38
Other Network Devices	39
Advanced Network Communications Topics	39
The OSI Model	39
Media Access Control (MAC) Addresses	40
Summary	41
Test Your Skills	41
Chapter 3: Cyber Stalking, Fraud, and Abuse	48
Introduction	48
How Internet Fraud Works	49
Investment Offers	49
Auction Frauds	51
Identity Theft	53
Phishing	55
Cyber Stalking	55
Laws about Internet Fraud	57
Protecting Yourself against Cyber Crime	58
Protecting against Investment Fraud	58
Protecting against Identity Theft	58
Secure Browser Settings	59

Summary	64
Test Your Skills	64
Chapter Footnotes	71
Chapter 4: Denial of Service Attacks	72
Introduction	72
Denial of Service	72
Illustrating an Attack	73
Common Tools Used for DoS	75
DoS Weaknesses	76
Specific DoS attacks	76
Land Attack	80
Distributed Denial of Service (DDoS)	81
Summary	85
Test Your Skills	85
Chapter 5: Malware	92
Introduction	92
Viruses	93
How a Virus Spreads	93
Recent Virus Examples	94
W32/Netsky-P	94
Troj/Invo-Zip	95
MacDefender	95
The Sobig Virus	95
The Mimail Virus	96
The Bagle Virus	97
A Nonvirus Virus	97
Rules for Avoiding Viruses	98
Trojan Horses	98
The Buffer-Overflow Attack	100
The Sasser Virus/Buffer Overflow	101

Spyware	101
Legal Uses of Spyware	102
How Is Spyware Delivered to a Target System?	102
Obtaining Spyware Software	102
Other Forms of Malware	104
Rootkit	104
Malicious Web-Based Code	105
Logic Bombs	106
Spam	106
Detecting and Eliminating Viruses and Spyware	107
Antivirus Software	107
Antispyware Software	108
Summary	110
Test Your Skills	110
Chapter 6: Techniques Used by Hackers	116
Introduction	116
Basic Terminology	117
The Reconnaissance Phase	117
Passive Scanning Techniques	117
Active Scanning Techniques	118
Actual Attacks	123
SQL Script Injection	123
Cross-Site Scripting	124
Password Cracking	125
Summary	127
Test Your Skills	127
Chapter 7: Industrial Espionage in Cyberspace	132
Introduction	132
What Is Industrial Espionage?	133
Information as an Asset	134
Real-World Examples of Industrial Espionage	136

Example 1: VIA Technology	137
Example 2: General Motors	137
Example 3: Interactive Television Technologies, Inc.	137
Example 4: Bloomberg, Inc.	138
Example 5: Avant Software	138
Industrial Espionage and You	138
How Does Espionage Occur?	139
Low-Tech Industrial Espionage	139
Spyware Used in Industrial Espionage	142
Steganography Used in Industrial Espionage	142
Phone Taps and Bugs	143
Protecting against Industrial Espionage	143
Industrial Espionage Act	146
Spear Phishing	146
Summary	147
Test Your Skills	147
Chapter 8: Encryption	154
Introduction	154
Cryptography Basics	155
History of Encryption	155
The Caesar Cipher	157
Multi-Alphabet Substitution	161
Binary Operations	162
Modern Methods	164
Single-Key (Symmetric) Encryption	164
Public Key (Asymmetric) Encryption	166
Legitimate Versus Fraudulent Encryption Methods	168
Digital Signatures	169
Hashing	169
Authentication	169

Encryptions Used in Internet	170
Virtual Private Networks	170
PPTP	171
L2TP	171
IPsec	171
Summary	172
Test Your Skills	172
Chapter 9: Computer Security Software	178
Introduction	178
Virus Scanners	179
How Does a Virus Scanner Work?	179
Virus-Scanning Techniques	180
Commercial Antivirus Software	181
Firewalls	182
Benefits and Limitation of Firewalls	182
Firewall Types and Components	182
How Firewalls Examine Packets	184
Firewall Configurations	184
Commercial and Free Firewall Products	185
Firewall Logs	187
Antispyware	187
Intrusion-Detection Software	187
IDS Categorization	188
IDS Approaches	189
Snort	189
Honey Pots	193
Other Preemptive Techniques	194
Summary	195
Test Your Skills	195

Chapter 10: Security Policies	200
Introduction	200
What Is a Policy	201
Defining User Policies	201
Passwords	202
Internet Use	203
Email Usage	204
Installing/Uninstalling Software	205
Instant Messaging	205
Desktop Configuration	206
Final Thoughts on User Policies	206
Defining System Administration Policies	207
New Employees	208
Departing Employees	208
Change Requests	209
Security Breaches	210
Virus Infection	210
Denial of Service Attacks	211
Intrusion by a Hacker	211
Defining Access Control	212
Developmental Policies	213
Standards, Guidelines, and Procedures	213
Summary	214
Test Your Skills	214
Chapter 11: Network Scanning and Vulnerability Scanning	220
Introduction	220
Basics of Assessing a System	221
Patch	221
Ports	222
Protect	225

Policies	226
Probe	228
Physical	228
Securing Computer Systems	229
Securing an Individual Workstation.	230
Securing a Server	231
Securing a Network	233
Scanning Your Network.	235
MBSA	235
NESSUS	238
Getting Professional Help	243
Summary	247
Test Your Skills.	247
Chapter 12: Cyber Terrorism and Information Warfare	254
Introduction	254
Actual Cases of Cyber Terrorism	255
China Eagle Union.	256
Economic Attacks	256
Military Operations Attacks.	258
General Attacks	259
Supervisory Control and Data Acquisitions	260
Information Warfare	260
Propaganda.	260
Information Control.	261
Disinformation.	263
Actual Cases	263
Future Trends	266
Positive Trends	267
Negative Trends	268

Defense against Cyber Terrorism	269
Summary	271
Test Your Skills	271
Chapter 13: Cyber Detective	276
Introduction	276
General Searches	277
Court Records and Criminal Checks	280
Sex Offender Registries	281
Civil Court Records	282
Other Resources	284
Usenet	285
Summary	287
Test Your Skills	287
Chapter 14: Introduction to Forensics	292
Introduction	292
General Guidelines	293
Don't Touch the Suspect Drive	293
Document Trail	294
Secure the Evidence	294
FBI Forensics Guidelines	294
Finding Evidence on the PC	295
Finding Evidence in the Browser	296
Finding Evidence in System Logs	296
Windows Logs	296
Linux Logs	297
Getting Back Deleted Files	298

Operating System Utilities	300
Net Sessions.....	300
Openfiles	300
Fc.....	301
Netstat.....	301
The Windows Registry	301
Summary	303
Test Your Skills.....	303
Appendix A: Glossary	306
Appendix B: Resources	312
General Computer Crime and Cyber Terrorism.....	312
General Knowledge	312
Cyber Stalking	312
Identity Theft	313
Port Scanners and Sniffers.....	313
Password Crackers	313
Countermeasures	313
Spyware	313
Counter Spyware.....	314
Cyber Investigation Tools	314
General Tools	314
Virus Research.....	315
Index	316

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 were 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 were 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 Commission⁵ (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 Justice⁷ 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 were 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.

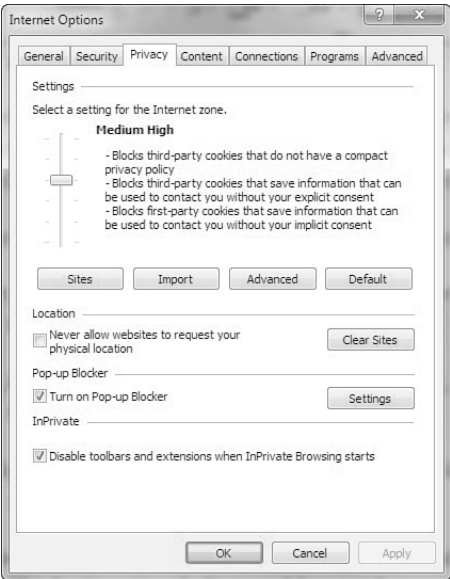


FIGURE 3.2 Internet Explorer privacy options.

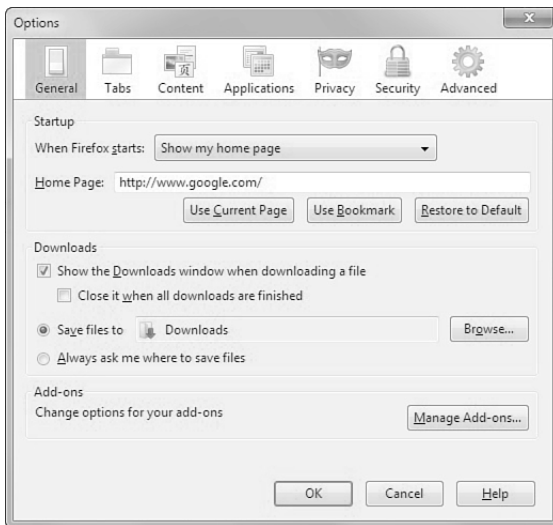


FIGURE 3.3 Firefox options.

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

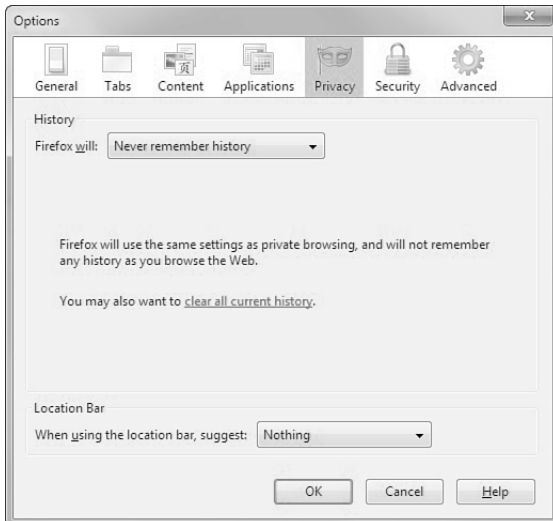


FIGURE 3.4 Firefox privacy.

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.

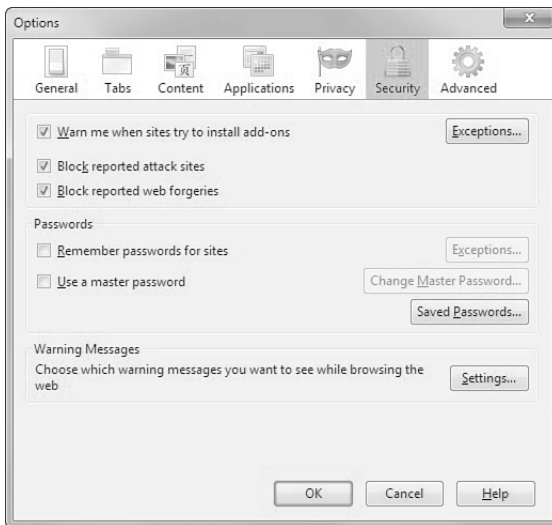


FIGURE 3.5 Firefox security.

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.safetynet.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.com: 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

3DES, 165

2600 magazine, 116

A

Absolute Keylogger, 103

access control, defining, 212-213

active code scanning, 181

active sessions, listing, 300

Address Resolution Protocol (ARP), 40

Adlema, Len, 167

administration policies

change requests, 209

defining, 207-209

departing employees, 208

new employees, 208

Advanced Encryption Standard, 165

adware, 4

algorithms, 164

AND binary operations, 162

anomaly detection (IDS), 188

Anonymous hacker group, 83

antispware software, 108-109

antistalking laws, 55-57

antivirus software, 107-108, 181

limitations, 200

apache2/* (Linux), 297

Application log, 296

applications gateways, 182-183

apport.log (Linux), 297

ARP (Address Resolution Protocol), 40

ARPANET (Advanced Research Projects Agency Network), 34

ASCII (American Standard Code for Information Interchange), 158

converting to, 158-161

decimal values, 159-160

hexidecimal values, 160-161

Assange, Julian, 83

assessing systems, 220-221

patches, 221

physical security, 228-229

policies, 226-228

ports, 222-225

probing, 228

protection, 225-226

asset identification worksheet, 135

asymmetric cryptography, 155

public-key, 166-168

attachments, 205

scanning, 180

attacks, 92, 104, 110, 123

assessing, 3-4

assessing likelihood, 7-8

buffer-overflow attacks, 100

cross-site scripting, 124

cyber terrorism, 254-256, 259-260, 271

China Eagle Union, 256

defending against, 269-270

economic attacks, 256-258

future trends, 266-268

military operations attacks, 258-259

negative trends, 268-269

DDoS attacks, buffer overflows, 75

detecting ongoing, 300-301

DNS poisoning, 5-7

DoS (Denial of Service), 5-7, 72-76, 81, 85

Anonymous hacker group, 83

buffer overflows, 73-75

change control, 211

command tools, 75-76

DDoS attacks, 81

defending against, 83-84

echo/chargen attacks, 81

ICMP flood attacks, 80

land attacks, 80

MyDoom attack, 81-82

PoD (ping of death) attacks, 80

Smurf IP attacks, 78-79

SYN floods, 76-78

teardrop attacks, 80

UDP flood attacks, 79

weaknesses, 76

finding live, 300

identifying, 4-5

information warfare, 260-266

future trends, 266-268

information control, 261-263

negative trends, 268-269

propaganda, 260-261

logic bombs, 106

malicious web-based code, 105-106

malware, 4-6

DoS (denial of service) attacks, 5-7

key loggers, 6

logic bombs, 6

session hijacking, 5-7

spyware, 5

system security breaches, 5-6

Trojan horses, 5

viruses, 5

web attacks, 5-7

password cracking, 125

OphCrack, 125-127

- rootkits, 104-105
- spam, 106
- spyware, 101-102
 - delivery of, 102
 - detecting and eliminating, 107-108
 - legal uses, 102
 - obtaining, 102-104
- SQL script injection, 123-124
- Trojan horses, 98-100
- viruses, 93-94
 - avoiding, 98
 - Bagle, 97
 - detecting and eliminating, 107-109
 - MacDefender, 95
 - Mimail, 96
 - Morris, 97
 - nonvirus viruses, 97
 - propagation, 93-94
 - Sasser, 101
 - Sobig, 95-96
 - Troj/Invo-Zip, 95
 - variants, 96
 - W32/Netsky-P, 94
- auctions, fraud, 51-53**
 - bid shielding, 52-53
 - bid siphoning, 53
 - shill bidding, 52-53
- auditing, 11**
- authentication, 10, 169-170**
- Avant Software corporate espionage case, 138**
- AVG AntiVirus, 181**
- AVG virus scanner, 98**
- Aykroyd, Dan, 9**

B

- Back Orifice, 99**
- backbones, 28**

background checks, 277, 284-287

- civil court records, 282-283
- sex offender registries, 281-282
- Usenet, 285-286
- background checks, employees, 144**
- BackTrack, 293**
- backup media, handling, 232**
- Bagle virus, 97**
- Bellaso, Giovan Battista, 162**
- Berners-Lee, Tim, 34**
- bid shielding, 52-53**
- bid siphoning, 53**
- binary numbers, converting, 29**
- binary operations, 162-164**
- BitLocker, 144**
- black hat hackers, 8, 116-117**
- block ciphers, 165**
- blocking ICMP packets, 83-84**
- Bloomberg, Inc. corporate espionage case, 138**
- Bloomberg, Michael, 138**
- blowfish symmetric block cipher, 165**
- Briney, Andrew, 142**
- Broadband Guide, 225**
- browsers**
 - configuring, 59-64
 - finding evidence in, 296
- buffer overflows, 73-75**
- buffer-overflow attacks, 100**
 - Sasser, 101
- bugs, 143**
- Bureau of Federal Prisons, 285**

C

cables, 23-24

- Category 5 cable, 24-25
- Category 6 cable, 24-25
- unshielded twisted-pair cable (UTP), 24

Caesar cipher, 157-161

Cain and Abel enumeration tool, 122

categorization, IDS (Intrusion Detection Software), 188-194

anomaly detection, 188

host-based, 189

misuse detection, 188

network-based, 189

passive systems, 188

reactive systems, 188

Category 5 cable, 24-25

Category 6 cable, 24-25

CDs, melting, 144

Center for Internet Security, 229

Cerf, Vince, 34

CERT (Computer Emergency Response Team), 14

creation of, 97

***CERT Information Assurance on Small Organizations* workbook, 135**

Certified Ethical Hacker tests, 8, 245

Certified Information Systems Security Professional (CISSP), 245

Certified Novel Engineer (CNE), 244

chain of custody, 294

Challenge Handshake Authentication Protocol (CHAP), 170

Chang, Jeremy, 137

change control, 209-210

DoS (Denial of Service) attacks, 211

hacker intrusion, 211-212

security breaches, 210

virus infection, 210-211

change requests, administration policies, 209

CHAP (Challenge Handshake Authentication Protocol), 170

checklists, policies, 228

Chinese Eagle Union, 264

CIA triangle, 11

CIDR (Classless Interdomain Routing), 30-31

cipher text, 164

circuit-level gateways, 182-184

CISSP (Certified Information Systems Security Professional), 245

Citrix application gateway, 226

civil court records, 282-283

classes, networks, 29-31

client errors, 33

CNE (Certified Novel Engineer), 244

command tools, DoS attacks, 75-76

commands

fc, 301

IPConfig, 35-37

Netcap, 293

netstat, 301

ping, 32, 36-38, 83

DDoS attacks, 75

DoS attacks, 73-75

Snort, 193

traceroute, 32, 83

tracert, 38

Computer Emergency Response Team (CERT), 14

creation of, 97

computer forensics, 292-294, 303

documentation, 294

FBI guidelines, 294-295

operating system utilities, 300-301

PCs, 295-296

recovering deleted files, 298-299

securing evidence, 294

system logs, 296-297

Windows Registry, 301-302

Computer Fraud and Abuse Act, 97

Computer Security Act, 13

configuration

browsers, 59-64

desktop, user policies, 206

firewalls, 184-185

connect scans, 119**connection types, Internet, 26****contact information, finding, 277-280****converting decimal numbers, 29****cookies**

- RST, 78
- spyware, 5
- SYN, 77

corporate espionage, 132-133, 138-139, 147

- Avant Software, 138
- Bloomberg, Inc., 138
- bugs, 143
- GM (General Motors), 137
- Industrial Espionage Act, 146
- information as asset, 134-136
- Interactive Television Technologies, Inc., 137-138
- low-tech, 139-142
- phone taps, 143
- protecting against, 143-146
- spear phishing, 146
- spyware, 142
- steganography, 142
- VIA Technology, 137

Counterexploitation website, 102-103**crackers, 116-117****cracking, 6**

- passwords, 125
- OphCrack, 125-127

criminal checks, 284-285, 287

- civil court records, 282-283
- sex offender registries, 281-282
- Usenet, 285-286

cross-site scripting, 124**cryptography, 155-157, 164, 168-170**

- algorithms, 164
- authentication, 169-170
- binary operations, 162-164
- Caesar cipher, 157-161

cipher text, 164

DES (Data Encryption Standard), 164-165

digital signatures, 169

fraudulent, 168

hashing, 169

keys, 164

multi-alphabet substitution, 161-162

plain text, 164

public-key encryption, 166-168

single-key encryption, 164-165

VPNs (virtual private networks), 170-171

IPsec (Internet Protocol Security), 171

L2TP (Layer 2 Tunneling Protocol), 171

PPTP (Point-to-Point Tunneling Protocol), 171

Cryptography.org, 156**cyber stalking, 55-57****cyber terrorism, 82, 254, 271**

- China Eagle Union, 256
- defending against, 269-270
- economic attacks, 256-258
- future trends, 266-268
- military operations attacks, 258-259
- negative trends, 268-269

Cybersecurity Research and Education Act of 2002, 267-268**Cyberterrorism Preparedness Act of 2002, 267**

D**DARPA (Defense Advanced Research Projects Agency), 34****Data Encryption Standard (DES), 164-165****data transmission, 26-27****DDoS (Distributed Denial of Service) attacks, buffer overflows, 75****DDoS attacks, 81**

- Anonymous hacker group, 83

decimal numbers, converting, 29

decimal values, ASCII, 159-160

Default Shares Registry setting, 233

Defense Advanced Research Projects Agency (DARPA), 34

defining

access control, 212-213

administration policies, 207-209

user policies, 201-207

deleted files, recovering, 298-299

denial of service (DoS) attacks. See DoS (denial of service) attacks

departing employees, administration policies, 208

DES (Data Encryption Standard), 164-165

desktop configuration, user policies, 206

developmental policies, 213

digital signatures, 169

disinformation campaigns, 263

Disk Digger, 298

disks, melting, 144

DNS (Domain Name System), 27, 34

poisoning, 5-7

DNS servers, 40

documentation, computer forensics, 294

documents, shredding, 144

domestic economic terrorism, 82

DoS (Denial of Service) attacks, 5-8, 72-76, 81, 85

Anonymous hacker group, 83

buffer overflows, 73-75

change control, 211

command tools, 75-76

DDoS attacks, 81

defending against, 83-84

echo/chargen attacks, 81

ICMP flood attacks, 80

Low Earth Orbit Ion Cannon tool, 9

MyDoom attack, 81-82

PoD (ping of death) attacks, 80

Smurf IP attacks, 78-79

SYN floods, 76-77

micro blocks, 77

RST cookies, 78

stack tweaking, 78

SYN cookies, 77

teardrop attacks, 80

UDP flood attacks, 79

weaknesses, 76

downloads, scanning, 180

DSO connections, 26

dual-homed hosts, 185

Duronio, Roger, 106

E

eBay, auction fraud, 51

bid shielding, 52-53

bid siphoning, 53

shill bidding, 52-53

echo/chargen attacks, 81

economic cyber terrorism, 256-258

Edwards, John, 267

EliteWrapper, 99

Ellison, Larry, 138

email

attachments, 205

scanning, 180

user policies, 204-205

employees

background checks, 144, 277, 284-287

civil court records, 282-283

sex offender registries, 281-282

Usenet, 285-286

finding contact information, 277-280

encrypting hard drives, 144

encryption, 154-156, 164, 168-170

algorithms, 164

authentication, 169-170

binary operations, 162-164

Caesar cipher, 157-161

cipher text, 164

cryptography, 155

DES (Data Encryption Standard), 164-165

digital signatures, 169

fraudulent, 168

hashing, 169

keys, 164

multi-alphabet substitution, 161-162

plain text, 164

public-key, 166-168

single-key, 164-165

VPNs (virtual private networks), 170-171

IPsec (Internet Protocol Security), 171

L2TP (Layer 2 Tunneling Protocol), 171

PPTP (Point-to-Point Tunneling Protocol), 171

enumeration, 122-123

Error 404: File Not Found, 32

espionage, 132-133, 138-139, 147

Avant Software, 138

Bloomberg, Inc., 138

bugs, 143

GM (General Motors), 137

Industrial Espionage Act, 146

information as asset, 134-136

Interactive Television Technologies, Inc., 137-138

low-tech, 139-142

phone taps, 143

protecting against, 143-146

spear phishing, 146

spyware, 142

steganography, 142

VIA Technology, 137

Euler's totient, 167

evidence, computer forensics, securing, 294

expulsion, user policies, 207

F

F-Secure, 14

Facebook, 278, 280

faillog (Linux), 297

false positives, virus scanners, 181

FBI Computer Forensics, 292-295

FBI state registry of sex offenders, 281

fc command, 301

federal prison records, searching, 284

File Transfer Protocol (FTP), 27

files

comparing, 301

recovering deleted, 298-299

FIN scans, 120

Firefox, 226

Firefox browsers, configuring, 61-62

Firestarter packet-filtering application, 225

firewalls, 10, 39, 182-187

application gateways, 182-183

benefits, 182

choosing, 225-226

circuit-level gateways, 182-184

configurations, 184-185

dual-homed hosts, 185

examining packets, 184

limitations, 182

logs, 187

network host-based, 185

router-based, 185

screened hosts, 185

screening, 182-183

stateful packet inspection (SPI) firewall, 184

stateless packet inspection, 184

flags, Nmap, 120

forensics (computer), 292-294, 303

documentation, 294

FBI guidelines, 294-295

operating system utilities, 300-301

- PCs, 295-296
- recovering deleted files, 298-299
- securing evidence, 294
- system logs, 296-297
- Windows Registry, 301-302

ForwardedEvents log, 296

fraud, 48-49

- auctions, 51-53
 - bid shielding, 52-53
 - bid siphoning, 53
 - shill bidding, 52-53
- common schemes, 49-50
- identity theft, 53-54
 - phishing, 55
 - protecting against, 58-59
- investment advice, 50-51
- investment offers, 49
- laws, 57-58
- protecting against, 58
 - browser settings, 59-64

FTP (File Transfer Protocol), 27

G

GIAC (Global Information Assurance Certification), 245

GM (General Motors) corporate espionage case, 137

gray hat hackers, 9, 117

guidelines, security policies, 213

H

hackers, 8, 116

- Anonymous, 83
- black hat, 8, 116-117
- change control, 211-212
- China Eagle Union, 256
- gray hat, 9, 117
- hacktivists, 264

- script kiddies, 9, 117
- sneakers, 9-10
- target information, 276
- white hat, 8, 116-117

hacking, 5-6

- across-site scripting, 124
- password cracking, 125-127
- phreaking, 10, 117
- reconnaissance phase, 117
 - enumeration, 122-123
 - passive scanning, 117-119
 - port scanning, 119-121
 - vulnerability assessment, 121
- SQL script injection, 123-124

hacktivists, 264

hard drives, encrypting, 144

hardening systems, 230

hashing, 78, 169

heuristic scanning, 180

hexidecimal values, ASCII, 160-161

hiring professional help, 243-246

Home PC Firewall Guide, 225

honey pots, 193, 292

host-based systems (IDS), 189

hosts, 34

HTML (Hypertext Markup Language), 34

HTTP (Hypertext Transfer Protocol), 27, 34

hubs, 25

Hutchinson, Shawn Michael, 57

Hypertext Markup Language (HTML), 34

Hypertext Transfer Protocol (HTTP), 27, 34

I

ICMP (Internet Control Message Protocol), 27, 78

ICMP flood attacks, 80

ICMP packets

- blocking, 83-84
- DoS attacks, 83

identity theft, 53-54

- laws, 57-58
- phishing, 55
- protecting against, 58-59

Identity Theft and Assumption Deterrence Act, 57**IDS (Intrusion Detection Software), 10-12, 187-188, 292**

- anomaly detection, 188
- categorization, 188-194
- honey pots, 193
- host-based, 189
- misuse detection, 188
- network-based, 189
- passive systems, 188
- preemptive blocking, 189
- reactive systems, 188
- Snort, 189-193

IETF (Internet Engineering Task Force), 34**Igusa, Mitsuru "Mitch," 138****IM (Instant Messaging), user policies, 205-206****index.dat file, 296****industrial espionage, 132-133, 147**

- Avant Software, 138
- Bloomberg, Inc., 138
- bugs, 143
- GM (General Motors), 137
- Industrial Espionage Act, 146
- information as asset, 134-136
- Interactive Television Technologies, Inc., 137-138
- low-tech, 139-142
- phone taps, 143
- protecting against, 143-146
- spear phishing, 146
- spyware, 142
- steganography, 142
- VIA Technology, 137

Industrial Espionage Act, 146**infiltration, 194****Infobel, 279****information control, 261-262**

- disinformation, 263

Information Security magazine, 263**information warfare, 254-255, 260-263**

- information control, 261-266
 - disinformation, 263
 - future trends, 266-268
 - negative trends, 268-269
- propaganda, 260-261

installing software, policies, 205**Instant Messaging (IM), user policies, 205-206****Interactive Television Technologies, Inc. corporate espionage case, 137-138****Internet**

- connection types, 26
- origins, 33-35
- technology expansions, 3

Internet Control Message Protocol (ICMP), 27, 78**Internet Engineering Task Force (IETF), 34****Internet Explorer, configuring, 60****Internet fraud, 48-49**

- auctions, 51
 - bid shielding, 52-53
 - bid siphoning, 53
 - shill bidding, 52-53
- common schemes, 49-50
- identity theft, 53-54
 - phishing, 55
 - protecting against, 58-59
- investment advice, 50-51
- investment offers, 49
- laws, 57-58
- protecting against, 58
 - browser settings, 59-64

Internet Protocol Security (IPsec), 171
Internet Relay Chat (IRC), 27
Internet service providers (ISPs), 28
Internet usage, user policies, 203-204
intrusion detection, 194
Intrusion Detection Software (IDS). See IDS (Intrusion Detection Software)
intrusion deterrence, 194
investment advice and offers, fraud, 50-51
IP addresses, 28-29
IPConfig utility, 23, 35-37
IPsec (Internet Protocol Security), 171
IPv4, 28, 32
IPv6, 31-32
IRC (Internet Relay Chat), 27
ISDN connections, 26
ISPs (Internet service providers), 28

J

jdbgmgr.exe virus hoax, 97
Johnson, Jeffrey, 8
Julius Caesar, 158

K

Kaspersky antivirus software, 181
Kaspersky virus scanner, 98
Kerberos authentication, 170
kern.log (Linux), 297
key loggers, 6, 103
keys, 164
Knoppix, 293

L

L2TP (Layer 2 Tunneling Protocol), 171
land attacks, 80
laws
 Computer Fraud and Abuse Act, 97
 Computer Security Act, 13

 Cybersecurity Research and Education Act of 2002, 267-268
 Cyberterrorism Preparedness Act of 2002, 267
 Identity Theft and Assumption Deterrence Act, 57
 Industrial Espionage Act, 146
 Internet fraud, 57-58

Layer 2 Tunneling Protocol (L2TP), 171

layered security approach, 12

least privileges, 11, 143

legal issues, network security, 13-14

legal uses of spyware, 102

lighttpd/* (Linux), 297

LinkedIn.com, 278-280

Linksys, 225

Linux logs, 297

listing active sessions, 300

live attacks, detecting and finding, 300-301

logging, 235

logic bombs, 6, 106

Logon Registry setting, 233

logs

 firewalls, 187

 Linux, 297

 Windows, 296-297

loopback addresses (IPv6), 31

Lopez, Inaki, 137

Low Earth Orbit Ion Cannon tool, 9

low-tech industrial espionage, 139-142

lpr.log (Linux), 297

M

MAC addresses, 40

MacDefender virus, 95

mail.* (Linux), 297

malicious web-based code, 105-106

malware, 4-6, 92, 104, 110

 buffer-overflow attacks, 100

 DDoS attacks, buffer overflows, 75

DoS attacks, 5-7, 85

Anonymous hacker group, 83

buffer overflows, 73-75

command tools, 75-76

DDoS attacks, 81

defending against, 83-84

echo/chargen attacks, 81

ICMP flood attacks, 80

land attacks, 80

MyDoom attack, 81-82

PoD (ping of death) attacks, 80

Smurf IP attacks, 78-79

SYN floods, 76-78

teardrop attacks, 80

UDP flood attacks, 79

weaknesses, 76

key loggers, 6

logic bombs, 6, 106

malicious web-based code, 105-106

rootkits, 104-105

session hijacking, 5-7

spam, 106

spyware, 5, 101

delivery of, 102

detecting and eliminating, 107-108

legal uses, 102

obtaining, 102-104

system security breaches, 5-6

Trojan horses, 5, 98-100

viruses, 5, 93-94

avoiding, 98

Bagle, 97

detecting and eliminating, 107-109

MacDefender, 95

Mimail, 96

Morris, 97

nonvirus viruses, 97

propagation, 93-94

Sasser, 101

Sobig, 95-96

Troj/Invo-Zip, 95

variants, 96

W32/Netsky-P, 94

web attacks, 5-7

Manhattan Project-level government programs, 270**MBSA (Microsoft Baseline Security Analyzer), 235-238****McAfee antivirus software, 181****McAfee Personal Firewall, 226****McAfee virus scanner, 98****MCITP (Microsoft Certified Information Technology Professional), 244****Medico, Joseph, 57****micro blocks, SYN floods, 77****Microsoft Baseline Security Analyzer, 235-238****Microsoft Certified Information Technology Professional (MCITP), 244****Microsoft Security Advisor, 14****military operations cyber terrorism, 258-259****Mimail virus, 96****misuse detection (IDS), 188****Mitnick, Kevin, 6****mobile malicious code, 106****mono-alphabet substitution, 157-161****Morris, Robert Tappan, 97****Morris worm, 97****mudulo, 168****multi-alphabet substitution, 161-162****MyDoom, 259****MyDoom DoS attack, 81-82****MyDoom virus, 98-99****mysql.* (Linux), 297**

N**NAPs (network access points), 28****National Center for State Courts, 284****National Security Agency, 229**

Nessus, 238-243
Net Sessions utility, 300
NetBIOS, 27
Netcat command, 293
netstat utility, 301
network access points (NAPs), 28
network devices, 25, 39
network host-based firewalls, 185
network interface cards (NICs), 23
Network News Transfer Protocol (NNTP), 27
network protocols, 22
network scanning, 220
network security
 legal issues, 13-14
 threats, assessment, 3-4
network utilities, 35
 IPConfig, 35-37
 ping, 36-38
 tracert, 38
network-based systems (IDS), 189
networks
 cables, 23-24
 Category 5 cable, 24-25
 Category 6 cable, 24-25
 unshielded twisted-pair cable (UTP), 24
 classes, 29-31
 scanning, 235-243
 securing, 233-235
 VPNs (virtual private networks)
 encryption, 171
 vulnerabilities, 200
new employees, administration policies, 208
***New Hacker's Dictionary*, 10**
newsgroups (Usenet), 285-286
NICs (network interface cards), 23
Nmap, 119-121
 flags, 120
NNTP (Network News Transfer Protocol), 27

nodes, 34
noncompete agreements, 133
nondisclosure agreements, 137
nonvirus viruses, 97
Norton AntiVirus software, 107, 181
Norton Personal Firewall, 225
Norton virus scanner, 98

O

OC connections, 26
OMB Circular A-130, 13
ongoing attacks, detecting, 300-301
online auctions, fraud, 51
 bid shielding, 52-53
 bid siphoning, 53
 shill bidding, 52-53
online resources, 14
Open Systems Interconnection model, 39-40
Openfiles utility, 300
operating system utilities, computer forensics, 300-301
operating systems, updating, 84
OphCrack, 125-127
OR binary operations, 163
OSI model, 39-40
Outpost Firewall, 186, 226

P

Pacer, 284
packets, 26
 firewalls, examining, 184
PAP (Password Authentication Protocol), 170
passive scanning techniques, 117-119
passive systems (IDS), 188
passphrases, 227
Password Authentication Protocol (PAP), 170
password cracking, 125
 OphCrack, 125-127

passwords, 169, 235

- policies, 227

- user policies, 202-203

patches, 221**PCs, finding evidence on, 295-296****People Search (Yahoo!), 278-279****perimeter security approach, 11****PGP (Pretty Good Privacy), 166-167****phishing, 55**

- spear, 146

phishing websites, 5, 108**phone taps, 143****phreaking, 10, 117****physical security, 228-229****ping command, 32**

- DDoS attacks, 75

- DoS attacks, 73-75

ping method, 23**ping scans, 119****ping utility, 83****ping utility, 35-38****plain text, 164****PoD (ping of death) attacks, 80****Point-to-Point Tunneling Protocol (PPTP), 171****Poitier, Sydney, 9****policies, 214, 226-228**

- access control, defining, 212-213

- administration policies

 - change requests, 209

 - defining, 207-209

 - departing employees, 208

 - new employees, 208

- checklists, 228

- developmental policies, 213

- guidelines, 213

- passwords, 227

- procedures, 213

- scope, 227

- security, 201

- standards, 213

- user policies

 - defining, 201-207

 - desktop configuration, 206

 - email usage, 204-205

 - expulsion, 207

 - IM (Instant Messaging), 205-206

 - installing/uninstalling software, 205

 - Internet usage, 203-204

 - passwords, 202-203

 - termination, 207

POP3 (Post Office Protocol version 3), 27, 33**port scanning, 119-121****portable storage media, limiting, 144****ports, 25, 28**

- assessing, 222-225

- routers, 222

PPTP (Point-to-Point Tunneling Protocol), 171**preemptive blocking (IDS), 189****Pretty Good Privacy (PGP), 166-167****prison searches, 284****privileges**

- least, 11, 143

probing networks, 228**procedures, security policies, 213****professional help, hiring, 243, 245-246****propaganda, 260-261****propagation, viruses, 93-94****protocols, 22**

- ARP (Address Resolution Protocol), 40

- POP3 (Post Office Protocol version 3), 27, 33

- TCP/IP protocols, 27

proxy servers, 10, 39**public records, searching, 284****public-key encryption, 166-168**

Q-R

Ranum, Marcus, 263

RC4 encryption, 165

reactive systems (IDS), 188

Read Me files, patches, 221

reconnaissance phase, hacking, 117

- enumeration, 122-123

- passive scanning, 117-119

- port scanning, 119-121

- vulnerability assessment, 121

recovering deleted files, 298-299

Redford, Robert, 9

repeaters, 25

Rivest, Ron, 165, 167

RJ-11 jacks, 23

RJ-45 jacks, 23-25

rootkits, 104-105

router-based firewalls, 185

routers, 25

- ports, 222

routing, CIDR (Classless Interdomain Routing), 30-31

RSA encryption method, 167

RST cookies, SYN floods, 78

S

SAM (Security Accounts Manager) files, 169

sandbox, scanning, 180

SANS Institute, 14, 84, 229

Santa Cruz Operations (SCO), MyDoom attack, 81-82

Sasser virus, 99-101

scanning networks, 235-243

scareware, 95

Schneier, Bruce, 165

SCO (Santa Cruz Operations), MyDoom attack, 81-82

screened hosts, 185

screening firewalls, 182-183

script injection (SQL), 123-124

script kiddies, 9, 117

Secret Service, 292

Secure Sockets Layer (SSL), 170

security. *See also* security policies

- activities, 10

- approaches, 11-12

- authentication, 10

- breaches, change control, 210

- computer

 - patches, 221

 - policies, 226-228

 - ports, 222-225

 - probing, 228

 - protection, 225-226

- infiltration, 194

- intrusion detection, 194

- intrusion deterrence, 194

- overestimating dangers, 4

- reactive approaches, 3

- systems, 229-235

Security Accounts Manager (SAM) files, 169

security devices, 10

Security log, 296

security policies, 201, 214, 226-228

- access control, defining, 212-213

- administration policies

 - change requests, 209

 - defining, 207-209

 - departing employees, 208

 - new employees, 208

- checklists, 228

- developmental policies, 213

- guidelines, 213

- passwords, 227

- procedures, 213

- scope, 227

- standards, 213

- user policies
 - defining, 201-207
 - desktop configuration, 206
 - email usage, 204-205
 - expulsion, 207
 - IM (Instant Messaging), 205-206
 - installing/uninstalling software, 205
 - Internet usage, 203-204
 - passwords, 202-203
 - termination, 207
- security rules, 235**
- security software, 178**
 - antispware, 187
 - antivirus software, 181
 - firewalls, 182-187
 - IDS (Intrusion Detection Software), 187-194
 - virus scanners, 179-181
- security templates, 229**
- server errors, 33**
- servers**
 - housing, 228
 - proxy, 39
 - securing, 231-233
 - vulnerabilities, 200
- Services log, 296**
- session hijacking, 5-7**
- sex offender registries, 281-282**
- Shamir, Adi, 167**
- shill bidding, 52-53**
- shredding documents, 144**
- Simple Mail Transfer Protocol (SMTP), 27**
- single-key encryption, 164-165**
- Sinn Fein, 260-261**
- SMTP (Simple Transfer Protocol), 27**
- SMTP protocol, 33**
- Smurf IP attacks, 78-79**
- sneakers, 9-10**
- Sneakers, 9**
- Snort, 189-193**
- Sobig virus, 95-96**
- Sobig.E variant, 96**
- social engineering, 6**
- software**
 - antispware, 187
 - antivirus, 181
 - limitations, 200
 - firewalls, 182-187
 - IDS (Intrusion Detection Software), 187-194
 - security, 178
 - antispware, 187
 - antivirus software, 181
 - firewalls, 182-187
 - IDS (Intrusion Detection Software), 187-194
 - virus scanners, 179-181
 - updating patches, 84
 - virus scanners, 179-181
- spam, 106**
- SPAP (Shiva Password Authentication Protocol), 170**
- spear phishing, 146**
- SPI (stateful packet inspection) firewall, 184**
- spreading of viruses, 93-94**
- Spy Sweeper, 108**
- spyware, 4-7, 95, 101**
 - delivery of, 102
 - detecting and eliminating, 107-108
 - industrial espionage, 142
 - legal uses, 102
 - obtaining, 102-104
- Spyware Guide website, 103-104**
- SQL script injection, 123-124**
- SSL (Secure Sockets Layer), 170**
- Stacheldraht, 76**
- stack tweaking, SYN floods, 78**
- stalking (cyber), 55-57**
- standards, security policies, 213**
- Stanford University History of Cryptography website, 156**

stateful packet inspection (SPI) firewall, 184

stateless packet inspection firewall, 184

steganography, 142

stream ciphers, 165

subnetting, 30-31

Switchboard.com, 280

switches, 25

symmetric cryptography, 155

single-key, 164-165

SYN cookies, 77

SYN floods, 76-77

micro blocks, 77

RST cookies, 78

stack tweaking, 78

SYN cookies, 77

SYN scans, 120

system assessment, 220-221

patches, 221

physical security, 228-229

policies, 226-228

ports, 222-225

probing, 228

protection, 225-226

system logs, finding evidence on, 296-297

system security breaches, 5-6

systems

hardening, 230

securing, 229-235

T

T1 connections, 26

T3 connections, 26

tape backups, melting, 144

target systems, spyware, delivery of, 102

TCP/IP (Transmission Control Protocol/Internet Protocol), 27

teardrop attacks, 80

Telnet, 27

templates, security, 229

termination, user policies, 207

Texas sex offender search page, 281-282

TFN (Tribal Flood Network), 75

TFTP (Trivial File Transfer Protocol), 27

The Ultimates.com, 280

threats, 92, 104, 110

assessing likelihood, 7-8

assessment, 3-4

buffer-overflow attacks, 100

DDoS attacks, buffer overflows, 75

DNS poisoning, 5-7

DoS attacks, 72-76, 81, 85

Anonymous hacker group, 83

buffer overflows, 73-75

command tools, 75-76

DDoS attacks, 81

defending against, 83-84

echo/chargen attacks, 81

ICMP flood attacks, 80

land attacks, 80

MyDoom attack, 81-82

PoD (ping of death) attacks, 80

Smurf IP attacks, 78-79

SYN floods, 76-78

teardrop attacks, 80

UDP flood attacks, 79

weaknesses, 76

identifying, 4-5

logic bombs, 106

malicious web-based code, 105-106

malware, 4-6

DoS (denial of service) attacks, 5-7

key loggers, 6

logic bombs, 6

session hijacking, 5-7

spyware, 5

system security breaches, 5-6

Trojan horses, 5

viruses, 5

web attacks, 5-7

- rootkits, 104-105
- spam, 106
- spyware, 101-102
 - delivery of, 102
 - detecting and eliminating, 107-108
 - legal uses, 102
 - obtaining, 102-104
- Trojan horses, 98-100
- viruses, 93-94
 - avoiding, 98
 - Bagle, 97
 - detecting and eliminating, 107-109
 - MacDefender, 95
 - Mimail, 96
 - Morris, 97
 - nonvirus viruses, 97
 - propagation, 93-94
 - Sasser, 101
 - Sobig, 95-96
 - Troj/Invo-Zip, 95
 - variants, 96
 - W32/Netsky-P, 94
- 3DES, 165**
- Tiny Keylogger, 103**
- TLS (Transport Layer Security), 170**
- Tomlinson, Ray, 34**
- traceroute utility, 32, 83**
- tracert utility, 23, 35, 38**
- Transport Layer Security (TLS), 170**
- Tribal Flood Network (TFN), 75**
- Triple DES, 165**
- Trithmeus, Johannes, 142**
- Trivial File Transfer Protocol (TFTP), 27**
- Troj/Invo-Zip virus, 95**
- Trojan horses, 4-5, 98-100, 104**
 - Troj/Invo-Zip, 95
- Trucrypt, 144-145**
- 2600 magazine, 116**
- TypO key logger, 103**

U

- UDP flood attacks, 79**
- Ugray, Zolt, 8**
- uniform resource locators (URLs), 32**
- uninstalling software, policies, 205**
- United Kingdom, public records, 284**
- United States Secret Service, 292**
- UNIX operating system, 34**
- unshielded twisted-pair cable (UTP), 24**
- URLs (uniform resource locators), 32**
- Usenet, 285-286**
- user policies**
 - defining, 201-207
 - desktop configuration, 206
 - email usage, 204-205
 - expulsion, 207
 - IM (Instant Messaging), 205-206
 - installing/uninstalling software, 205
 - Internet usage, 203-204
 - passwords, 202-203
 - termination, 207
- user.log (Linux), 297**
- utilities**
 - computer forensics, 300-301
 - fc, 301
 - IPConfig, 35-37
 - Net Sessions, 300
 - netstat, 301
 - network, 35
 - Openfiles, 300
 - ping, 36-38, 83
 - DDoS attacks, 75
 - DoS attacks, 73-75
 - traceroute, 83
 - tracert, 38
- UTP (unshielded twisted-pair cable), 24**

V

variants, viruses, 96

VIA Technology corporate espionage case, 137

Vigenère cipher, 162

virtual private networks (VPNs). See VPNs (virtual private networks)

virulence, 95

virus infection, change control, 210-211

virus scanning software, 98, 107-109, 179-181

 false positives and negatives, 181

 updating, 84

viruses, 4-5, 93-94

 avoiding, 98

 Bagle, 97

 detecting and eliminating, 107-109

 MacDefender, 95

 Mimail, 96

 Morris, 97

 nonvirus viruses, 97

 propagation, 93-94

 Sobig, 95-96

 Troj/Invo-Zip, 95

 variants, 96

 versus worms, 82, 99

 W32/Netsky-P, 94

VPNs (virtual private networks), encryption, 170-171

vulnerability assessment, 121

vulnerability scanning, 220

W

W32/Netsky-P virus, 94

war-dialing, 6

weaknesses, DoS attacks, 76

web attacks, 5-7

WebRoot Spy Sweeper, 108

white hat hackers, 8, 116-117

Whols, 27

WhoWhere.com, 280

Wikileaks, 83

Windows logs, 296-297

Windows Registry, computer forensics, 301-302

workstations, 229

 securing, 230-231

worms, 4

 Morris, 97

 versus viruses, 82, 99

X-Z

XOR binary operations, 163-164

Yahoo! People Search, 278-279

Yellow Pages, 280

Zero Spyware Removal, 108

Zezev, Oleg, 138

Zimmerman, Phil, 167

Zone Lab firewalls, 186

zone transfers, 40