

Table of Contents

Introduction ix

Chapter 1
An Introduction to High-Technology Crime 1

What Is High-Technology Crime? 2

- Computer Crimes 3
- Cybercrime 4
- Consolidating High-Technology Crimes 5

How Serious Is the High-Technology Crime Problem? 5

The Purpose of This Work 8

- The Criminal Acts 8
- Investigating High-Technology Crimes 12
- Introduction to Computer Forensics and the Future of Technology Crime 14

In the News 15

Review Questions 16

Online Resources 16

Chapter 2
Hackers, Crackers, and Phone Phreaks 17

The Evolution of the Term *Hacker* 18

The Introduction of Hacking to the Public 19

Types of Hackers 24

- Black-Hat Hackers 24
- White-Hat Hackers 24
- Gray-Hat Hackers 25
- Script Kiddies 25
- Hactivists 25
- Cyberterrorists 26

Hacker Technique and *Modus Operandi* 26

- Password Grabbers and Loggers 30
- Blue Boxing Programs 30
- War-Dialers 31
- Encryption Software 32
- Password Recovery Software 32
- BIOS Password Crackers 33

Security Vulnerability to Scanners	33
Packet Sniffers	34
Operating System Password Crackers	34
War-Driver Programs (Wireless Network Scanners)	35
Hacker Attack Techniques	36
Data Manipulation	37
Trojan Horses	38
Computer Viruses	39
Denial-of-Service Attacks	39
IP Spoofing	40
Web Spoofing	41
Non-Software/Non-Network-Based Attacks	42
The Crime of Phreaking	42
How Phreakers Operate	46
Cellular Phone Phreaking	47
Calling Card Fraud	48
Call Sell Services	49
The Hacker/Phreaker Subculture	49
The Hacker Ethic	50
The Hacker Language	52
Hacker Conferences	55
Conclusion	55
In the News	57
Review Questions	57
Further Reading	58
Online Resources	59

Chapter 3

Identity Theft: Tools and Techniques of 21st-Century Bandits

61

How Serious Is the Identity Theft Problem?	63
How Identity Thieves Operate	65
Dumpster Diving	67
Skimming	68
Shoulder Surfing	69
Retail Scams	70
Packet Sniffing	71
Phishing	72
Anti-Identity Theft Legislation	73
Responses to Identity Theft	74
Conclusion	76
In the News	77
Review Questions	78
Further Reading	79
Online Resources	79

Chapter 4

Digital Child Pornography and the Abuse of Children in Cyberspace**81**

The Grooming Process	83
Friendship Phase	84
Secrecy Phase	84
Physical Contact Phase	85
Pornography Phase	85
Child Pornography and the Internet	86
Early Methods of Child Pornography Distribution	88
The Criminal Justice System's Response to Digital Child Pornography	90
The Evolution of Anti-Child Pornography Legislation	91
The Supreme Court and Child Pornography Investigations	92
Combating Child Pornography	94
Current Issues in Child Pornography—The Sexting Phenomenon	96
Conclusion	97
In the News	99
Review Questions	99
Further Reading	100
Online Resources	100

Chapter 5

Financial Fraud and Con Artistry on the Internet**101**

Online Auction Fraud	102
Buying Wives and Prostitutes Online	106
Mail-Order Bride Services	107
Mail-Order Bride Fraud	109
Mail-Order Bride Agency Fraud	111
Legal Issues Involving Mail-Order Brides	112
Prostitution Online	113
Use of Internet by Customers	114
The Internet and Prostitution	116
Nigerian 419 Schemes—Fraud Schemes Based on Greed	120
Phishing—Seeking Out Passwords and Financial Information	122
Conclusion	123
In the News	125
Review Questions	126
Further Reading	126
Online Resources	126

Chapter 6

Online Harassment and Cyberstalking**129**

Online Harassment	129
Cyberstalking	133

How Cyberstalkers Operate	135
The Criminal Justice Response to Cyberstalking	138
Conclusion	140
In the News	142
Review Questions	142
Further Reading	143
Online Resources	143

Chapter 7

Intellectual Property Theft and Digital File Sharing **145**

History of Peer-to-Peer Networking	147
Legal Responses to the File-Sharing Problem	150
Alternative Methods Employed by the RIAA and MPAA	153
The Current State of File Sharing	154
Conclusion	156
In the News	158
Review Questions	158
Further Reading	159
Online Resources	159

Chapter 8

Investigating on the Web: Examining Online Investigations and Sting Operations **161**

Locating a Suspect on the Internet	161
Locating Information from E-Mails	164
Examining an E-Mail Header	166
Online Investigations: Proactive versus Reactive	168
The "Dateline Phenomenon"	172
Conclusion	173
In the News	174
Review Questions	175
Further Reading	175
Online Resources	175

Chapter 9

Seizure of Digital Evidence **177**

The Search Warrant Requirement	177
Preplanning for the Search Warrant	180
Planning for the Seizure of Electronic Communications	183
Warrantless Search Doctrines and Technological Evidence	185
The Expectation of Privacy	186
Warrantless Consent Searches	187
Searches Based on Exigent Circumstances	190
Searches Incident to a Lawful Arrest	192
Plain-View Seizures	195

Warrantless Searches by a Private Party	198
Miscellaneous Warrantless Search Doctrines	199
Conclusion	201
In the News	202
Review Questions	202
Further Reading	203
Online Resources	203

Chapter 10

Executing a Search Warrant for Digital Evidence **205**

The Steps of Executing a Search Warrant for Digital Evidence	206
Step One: Removing the Suspect from the Computer	206
Step Two: Securing the Scene	207
Step Three: Disconnect Any Outside Control Possibilities	209
Step Four: Powering Down the Computer	210
Step Five: Disassembling the Computer	218
Step Six: Securing Additional Evidence from the Scene	220
Step Seven: Preparing the Evidence for Transportation	222
Wrapping Up the Search and Preserving the Evidence	223
Understanding the Chain of Custody	223
Conclusion	224
In the News	226
Review Questions	226
Further Reading	227
Online Resources	227

Chapter 11

An Introduction to Computer Forensics **229**

What Is Computer Forensics?	229
How Computers Store Data	230
Internet Activity Stored on a Computer	232
The Computer Forensics Process	234
Verifying Files and File Signatures	236
The Forensic Analysis	239
The Forensics Report	240
Computer Forensic Software Packages	240
EnCase	241
Forensic Tool Kit	241
Non-GUI-Based Software Utilities	242
Admissibility of Digital Evidence	243
The Authentication and Admission of Digital Evidence at Trial	245
Conclusion	248
In the News	250
Review Questions	251
Further Reading	251
Online Resources	251

Chapter 12

The Future of High-Technology Crime

253

Cyberterrorism	253
What Acts Qualify as Cyberterrorism?	255
What Acts Are Not Cyberterrorism?	257
Evolution of the Legal System	257
The Globalization of Cybercrime	260
Conclusion	261
In the News	262
Review Questions	263
Further Reading	264
Online Resources	264

Chapter 13

An Introduction to Cybercriminology: What is Cybercriminology

265

Techniques of Neutralization and Rationalization	266
Further Reading	269
Social Structure and Social Learning Theory	269
Further Reading	271
Routine Activities Theory	272
Further Reading	273
Self-Control Theory—General Theory of Crime	274
Further Reading	275
Labeling Theory	275
Further Reading	276
Deindividuation Theory	277
Further Reading	280
Space Transition Theory	280
Further Reading	282
Conclusion	282
Review Questions	283
Online Resources	283

Bibliography 285

About the Author 301

Index 303