

Contents

Foreword	vii
About Dr. Kamlesh Bajaj	ix
About the Authors	xi
Preface	xiii
Acknowledgments	xvii
List of Figures	xxxiii
List of Tables	xxxix
List of Boxes	xliii

1	Introduction to Cybercrime	1
	Learning Objectives	1
1.1	Introduction	1
1.2	Cybercrime: Definition and Origins of the Word	1
1.3	Cybercrime and Information Security	13
1.4	Who are Cybercriminals?	16
1.5	Classifications of Cybercrimes	17
	1.5.1 E-Mail Spoofing	18
	1.5.2 Spamming	18
	1.5.3 Cyberdefamation	19
	1.5.4 Internet Time Theft	21
	1.5.5 Salami Attack/Salami Technique	21
	1.5.6 Data Diddling	21
	1.5.7 Forgery	22
	1.5.8 Web Jacking	22
	1.5.9 Newsgroup Spam/Crimes Emanating from Usenet Newsgroup	22
	1.5.10 Industrial Spying/Industrial Espionage	22
	1.5.11 Hacking	23
	1.5.12 Online Frauds	23
	1.5.13 Pornographic Offenses	27
	1.5.14 Software Piracy	28
	1.5.15 Computer Sabotage	28
	1.5.16 E-Mail Bombing/Mail Bombs	30
	1.5.17 Usenet Newsgroup as the Source of Cybercrimes	30
	1.5.18 Computer Network Intrusions	30
	1.5.19 Password Sniffing	30
	1.5.20 Credit Card Frauds	31
	1.5.21 Identity Theft	31
1.6	Cybercrime: The Legal Perspectives	32
1.7	Cybercrimes: An Indian Perspective	32

1.8	Cybercrime and the Indian ITA 2000	34
	1.8.1 <i>Hacking and the Indian Law(s)</i>	34
1.9	A Global Perspective on Cybercrimes	36
	1.9.1 <i>Cybercrime and the Extended Enterprise</i>	38
1.10	Cybercrime Era: Survival Mantra for the Netizens	39
1.11	Concluding Remarks and Way Forward to Further Chapters	39
	Summary	40
	Review Questions	40
	References	40
	Further Reading	42
2	Cyberoffenses: How Criminals Plan Them	45
	Learning Objectives	45
2.1	Introduction	45
	2.1.1 <i>Categories of Cybercrime</i>	48
2.2	How Criminals Plan the Attacks	49
	2.2.1 <i>Reconnaissance</i>	50
	2.2.2 <i>Passive Attacks</i>	50
	2.2.3 <i>Active Attacks</i>	54
	2.2.4 <i>Scanning and Scrutinizing Gathered Information</i>	58
	2.2.5 <i>Attack (Gaining and Maintaining the System Access)</i>	61
2.3	Social Engineering	61
	2.3.1 <i>Classification of Social Engineering</i>	62
2.4	Cyberstalking	65
	2.4.1 <i>Types of Stalkers</i>	66
	2.4.2 <i>Cases Reported on Cyberstalking</i>	66
	2.4.3 <i>How Stalking Works?</i>	66
	2.4.4 <i>Real-Life Incident of Cyberstalking</i>	67
2.5	Cybercafe and Cybercrimes	67
2.6	Botnets: The Fuel for Cybercrime	71
	2.6.1 <i>Botnet</i>	71
2.7	Attack Vector	73
2.8	Cloud Computing	75
	2.8.1 <i>Why Cloud Computing?</i>	76
	2.8.2 <i>Types of Services</i>	77
	2.8.3 <i>Cybercrime and Cloud Computing</i>	77
	Summary	79
	Review Questions	79
	References	79
	Further Reading	80
3	Cybercrime: Mobile and Wireless Devices	81
	Learning Objectives	81
3.1	Introduction	81
3.2	Proliferation of Mobile and Wireless Devices	82

3.3	Trends in Mobility	84
3.4	Credit Card Frauds in Mobile and Wireless Computing Era	87
	3.4.1 <i>Types and Techniques of Credit Card Frauds</i>	88
3.5	Security Challenges Posed by Mobile Devices	91
3.6	Registry Settings for Mobile Devices	92
3.7	Authentication Service Security	93
	3.7.1 <i>Cryptographic Security for Mobile Devices</i>	93
	3.7.2 <i>LDAP Security for Hand-Held Mobile Computing Devices</i>	94
	3.7.3 <i>RAS Security for Mobile Devices</i>	95
	3.7.4 <i>Media Player Control Security</i>	98
	3.7.5 <i>Networking API Security for Mobile Computing Applications</i>	98
3.8	Attacks on Mobile/Cell Phones	99
	3.8.1 <i>Mobile Phone Theft</i>	99
	3.8.2 <i>Mobile Viruses</i>	101
	3.8.3 <i>Mishing</i>	101
	3.8.4 <i>Vishing</i>	102
	3.8.5 <i>Smishing</i>	103
	3.8.6 <i>Hacking Bluetooth</i>	105
3.9	Mobile Devices: Security Implications for Organizations	107
	3.9.1 <i>Managing Diversity and Proliferation of Hand-Held Devices</i>	107
	3.9.2 <i>Unconventional/Stealth Storage Devices</i>	108
	3.9.3 <i>Threats through Lost and Stolen Devices</i>	110
	3.9.4 <i>Protecting Data on Lost Devices</i>	111
	3.9.5 <i>Educating the Laptop Users</i>	111
3.10	Organizational Measures for Handling Mobile Devices-Related Security Issues	112
	3.10.1 <i>Encrypting Organizational Databases</i>	113
	3.10.2 <i>Including Mobile Devices in Security Strategy</i>	113
3.11	Organizational Security Policies and Measures in Mobile Computing Era	114
	3.11.1 <i>Importance of Security Policies relating to Mobile Computing Devices</i>	114
	3.11.2 <i>Operating Guidelines for Implementing Mobile Device Security Policies</i>	115
	3.11.3 <i>Organizational Policies for the Use of Mobile Hand-Held Devices</i>	116
3.12	Laptops	116
	3.12.1 <i>Physical Security Countermeasures</i>	117
	Summary	120
	Review Questions	121
	References	121
	Further Reading	122
4	Tools and Methods Used in Cybercrime	125
	Learning Objectives	125
4.1	Introduction	125
4.2	Proxy Servers and Anonymizers	129

4.3	Phishing	131
	4.3.1 <i>How Phishing Works?</i>	131
4.4	Password Cracking	132
	4.4.1 <i>Online Attacks</i>	134
	4.4.2 <i>Offline Attacks</i>	134
	4.4.3 <i>Strong, Weak and Random Passwords</i>	135
	4.4.4 <i>Random Passwords</i>	136
4.5	Keyloggers and Spywares	137
	4.5.1 <i>Software Keyloggers</i>	137
	4.5.2 <i>Hardware Keyloggers</i>	140
	4.5.3 <i>Antikeylogger</i>	140
	4.5.4 <i>Spywares</i>	140
4.6	Virus and Worms	143
	4.6.1 <i>Types of Viruses</i>	146
4.7	Trojan Horses and Backdoors	151
	4.7.1 <i>Backdoor</i>	152
	4.7.2 <i>How to Protect from Trojan Horses and Backdoors</i>	153
4.8	Steganography	155
	4.8.1 <i>Steganalysis</i>	158
4.9	DoS and DDoS Attacks	158
	4.9.1 <i>DoS Attacks</i>	158
	4.9.2 <i>Classification of DoS Attacks</i>	159
	4.9.3 <i>Types or Levels of DoS Attacks</i>	160
	4.9.4 <i>Tools Used to Launch DoS Attack</i>	161
	4.9.5 <i>DDoS Attacks</i>	162
	4.9.6 <i>How to Protect from DoS/DDoS Attacks</i>	163
4.10	SQL Injection	164
	4.10.1 <i>Steps for SQL Injection Attack</i>	165
	4.10.2 <i>How to Prevent SQL Injection Attacks</i>	167
4.11	Buffer Overflow	168
	4.11.1 <i>Types of Buffer Overflow</i>	168
	4.11.2 <i>How to Minimize Buffer Overflow</i>	170
4.12	Attacks on Wireless Networks	171
	4.12.1 <i>Traditional Techniques of Attacks on Wireless Networks</i>	176
	4.12.2 <i>Theft of Internet Hours and Wi-Fi-based Frauds and Misuses</i>	177
	4.12.3 <i>How to Secure the Wireless Networks</i>	179
	Summary	180
	Review Questions	181
	References	181
	Further Reading	183
5	Phishing and Identity Theft	185
	Learning Objectives	185
5.1	Introduction	185

5.2	Phishing	187
	5.2.1 <i>Methods of Phishing</i>	191
	5.2.2 <i>Phishing Techniques</i>	193
	5.2.3 <i>Spear Phishing</i>	195
	5.2.4 <i>Types of Phishing Scams</i>	196
	5.2.5 <i>Phishing Toolkits and Spy Phishing</i>	201
	5.2.6 <i>Phishing Countermeasures</i>	202
5.3	Identity Theft (ID Theft)	206
	5.3.1 <i>Personally Identifiable Information(PII)</i>	209
	5.3.2 <i>Types of Identity Theft</i>	211
	5.3.3 <i>Techniques of ID Theft</i>	218
	5.3.4 <i>Identity Theft: Countermeasures</i>	220
	5.3.5 <i>How to Efface Your Online Identity</i>	220
	Summary	221
	Review Questions	222
	References	222
	Further Reading	224
6	Cybercrimes and Cybersecurity: The Legal Perspectives	227
	Learning Objectives	227
6.1	Introduction	227
6.2	Cybercrime and the Legal Landscape around the World	230
	6.2.1 <i>A Broad View on Cybercrime Law Scenario in the Asia-Pacific Region</i>	231
	6.2.2 <i>Online Safety and Cybercrime Laws: Detailed Perspective on the Current Asia-Pacific Scenario</i>	233
	6.2.3 <i>Anti-Spam Laws in Canada</i>	243
	6.2.4 <i>Cybercrime and Federal Laws in the US</i>	245
	6.2.5 <i>The EU Legal Framework for Information Privacy to Prevent Cybercrime</i>	247
	6.2.6 <i>Cybercrime Legislation in the African Region</i>	249
6.3	Why Do We Need Cyberlaws: The Indian Context	253
6.4	The Indian IT Act	254
	6.4.1 <i>Admissibility of Electronic Records: Amendments made in the Indian ITA 2000</i>	264
	6.4.2 <i>Positive Aspects of the ITA 2000</i>	269
	6.4.3 <i>Weak Areas of the ITA 2000</i>	270
6.5	Challenges to Indian Law and Cybercrime Scenario in India	271
6.6	Consequences of Not Addressing the Weakness in Information Technology Act	272
6.7	Digital Signatures and the Indian IT Act	273
	6.7.1 <i>Public-Key Certificate</i>	273
	6.7.2 <i>Representation of Digital Signatures in the ITA 2000</i>	274
	6.7.3 <i>Impact of Oversights in ITA 2000 Regarding Digital Signatures</i>	275
	6.7.4 <i>Implications for Certifying Authorities</i>	277

	6.7.5 <i>The Current Scenario Regarding Digital Signatures under the Indian IT Act</i>	278
	6.7.6 <i>Cryptographic Perspective on the Indian IT Act</i>	279
6.8	Amendments to the Indian IT Act	282
	6.8.1 <i>Overview of Changes Made to the Indian IT Act</i>	283
	6.8.2 <i>Cybercafe-Related Matters Addressed in the Amendment to the Indian IT Act</i>	289
	6.8.3 <i>State Government Powers Impacted by the Amendments to the Indian IT Act</i>	293
	6.8.4 <i>Impact of IT Act Amendments on Information Technology Organizations</i>	295
6.9	Cybercrime and Punishment	305
6.10	Cyberlaw, Technology and Students: Indian Scenario	307
	Summary	309
	Review Questions	310
	References	311
	Further Reading	312
7	Understanding Computer Forensics	317
	Learning Objectives	317
7.1	Introduction	317
7.2	Historical Background of Cyberforensics	318
7.3	Digital Forensics Science	320
7.4	The Need for Computer Forensics	323
7.5	Cyberforensics and Digital Evidence	327
	7.5.1 <i>The Rules of Evidence</i>	329
7.6	Forensics Analysis of E-Mail	332
	7.6.1 <i>RFC2822</i>	338
7.7	Digital Forensics Life Cycle	339
	7.7.1 <i>The Digital Forensics Process</i>	339
	7.7.2 <i>The Phases in Computer Forensics/Digital Forensics</i>	341
	7.7.3 <i>Precautions to be Taken when Collecting Electronic Evidence</i>	353
7.8	Chain of Custody Concept	355
7.9	Network Forensics	357
7.10	Approaching a Computer Forensics Investigation	358
	7.10.1 <i>Typical Elements Addressed in a Forensics Investigation Engagement Contract</i>	359
	7.10.2 <i>Solving a Computer Forensics Case</i>	361
7.11	Setting up a Computer Forensics Laboratory: Understanding the Requirements	362
7.12	Computer Forensics and Steganography	368
	7.12.1 <i>Rootkits</i>	370
	7.12.2 <i>Information Hiding</i>	371
7.13	Relevance of the OSI 7 Layer Model to Computer Forensics	373
	7.13.1 <i>Step 1: Foot Printing</i>	373