



Updated  
for 2021

# CYBERHEIST

The Biggest Financial Threat  
Facing Organizations Worldwide

Stu Sjouwerman



# CYBERHEIST

**The Biggest Financial Threat Facing Organizations Worldwide**

Stu Sjouwerman



**Publisher/Lead Author**  
*Stu Sjouwerman*

**Contributing Authors**

*Naomi Alper  
Justin Korelc  
Kim Lindros  
Jeff T. Parker  
James Pyles  
Ed Tittel  
Michelle Zaval  
Richard G Lowe Jr  
Roger A. Grimes*

**Technical Editors**

*Richard G Lowe Jr  
Roger A. Grimes*

**Developmental Editor**

*Kim Lindros*

**Copyeditor**

*Kitty Wilson*

**Technical Editor**

*Darril Gibson*

**Compositor and Graphic Artist**

*Kim Eoff*

**Proofreader**

*Kim Lindros*

**Indexer**

*Liz Cunningham*

**Cover Design**

*David Brier, DBD International*

**Cover Art Photographer**

*Alan Poulson*

**Cover and Interior Printing and**

*Binding  
Globus Printing*

## **CYBERHEIST: The Biggest Financial Threat Facing Organizations Worldwide**

Copyright © 2011, 2016, 2020 KnowBe4.

All rights reserved. No part of this book may be reproduced or transmitted in any form or any manner, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without permission in writing from the publisher.

### **Trademarks**

Trademarked names appear throughout this book. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the publisher states that it is using the names for editorial purposes only and to the benefit of the trademark owner, with no intention of infringing upon that trademark.

### **Warning and Disclaimer**

Every effort has been made to make this book as complete and as accurate as possible, but no warranty of fitness is implied. The information provided is on an “as is” basis. The authors 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.

This book is also published in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

### **KnowBe4**

33 N Garden Ave, Suite 1200

Clearwater, Florida 33755

Toll Free: 855-KNOWBE4 (566-9234)

**[www.KnowBe4.com](http://www.KnowBe4.com)**

ISBN: 978-0-692-64431-7

Library of Congress Control Number: 2016933543

Published in North America by KnowBe4

10 9 8 7 6 5 4 3 2 1

This book is dedicated to all the sleepless cybercrime fighters in the world. You know who you are.

Thanks very much for what you do.



# Acknowledgments

This project was a true team effort. My sincere thanks to all the people who helped bring my ideas to a tangible, cohesive book. This includes the following contributors: Naomi Alpern, Justin Korelc, Kim Lindros, Jeff T. Parker, James Pyles, Ed Tittel, Richard Lowe Jr, and Michelle Zavala. Ed Tittel also designed and reviewed the original edition's entire contents. Roger A. Grimes updated, reviewed, and edited the 2020 edition's entire contents.

The production team included these fine people: Kitty Wilson, copy editor; Darril Gibson, technical editor; Kim Eoff, layout design, compositor, and artist; Liz Cunningham, indexer; and Kim Lindros, who wore several hats, including proofreader and project manager. David Brier, DBD International, did the cover design, and the cover art photographer was Alan Poulson.

A special and sincere thank you to Roger Grimes, who is the Executive Technical Editor of this version of *Cyberheist* as well as Data-Driven Defense Evangelist for KnowBe4. Grimes is a cybersecurity industry veteran with over 30 years of experience in computer security and a well-known author of 12 books. His input and expertise was instrumental in incorporating the accurate technical aspects of this latest version of the book.

My sincere thanks to everyone who ever worked at Sunbelt Software and who helped to make us the Inc. 500 success that we were. That was a great run!





# About the Author

Stu Sjouwerman (pronounced “shower-man”) has been in Information Technology for 40+ years, the last 20+ of which were in IT Security. Stu has founded several successful computer security companies, including KnowBe4, Inc. and Sunbelt Software. KnowBe4 is the world’s leading provider of security awareness training and simulated phishing, helping organizations improve their cultures to prevent social engineering and other cybersecurity incidents. KnowBe4 is valued at over \$1 billion dollars and has over 30,000 customers. It has been selected as a primary leader of technology and thought leadership by dozens of industry publications. KnowBe4 has won multiple “best place to work” culture awards.

As a co-founder of Inc. 500 company Sunbelt Software, he has been specializing in antispyware products since 2003. A few years later, Sunbelt developed antivirus software, integrated a firewall, and at the same time, developed antispam software for both consumers and enterprises. In 2010, Sunbelt was sold to GFI software, a portfolio company of Insight Partners, a \$3 billion Boston-based hedge fund.

This is Stu’s fourth book. He has co-authored three books about Windows system administration, the first being *Windows NT Power Toolkit*. Released in October 1999, this book reached #4 on Amazon.com’s USA bestseller list the first week of its release and #1 in the UK. In 2003, a new book about Windows XP was published. The second and third books also reached Amazon’s Top 10 List.

From 1996 through 2011, Stu was the Editor-In-Chief of WServer News, an email newsletter to 100,000+ IT system administrators, which helped them to keep their systems secure. Stu also served as editor of GFI Media Services, which published four major online newsletters, including WServer News, WXP News, Win7 News, and GFI Security News. Stu is currently Editor-in-Chief of Cyberheist News, an e-zine tailored to deliver IT security news, technical updates and social engineering alerts to IT professionals.

He lives in the Tampa Bay, Florida area with his wife Rebecca and their three cats.



# Table of Contents

<b>Acknowledgments</b>	<b>i</b>
<b>About the Author</b>	<b>iii</b>
<b>Table of Contents</b>	<b>v</b>
<b>List of Tables</b>	<b>xiii</b>
<b>List of Figures</b>	<b>xv</b>
<b>Preface</b>	<b>xvii</b>
About This Book	xvii
Special Elements Used in This Book	xviii
Contact Us	xviii
<b>Part 1 The Business of Cybercrime</b>	<b>1</b>
<b>Chapter 1 What Drives Cybercrime?</b>	<b>3</b>
What Exactly Is Cybercrime?	4
Who's a Target for Cybercrime?	5
A Million Stories for a Million Scams	9
A Case of Criminal Culture	11
Cybercrime Learning and Lore	12
Variations on a Scamming Theme	13
Internet, and the Money Is Easy	14
Offshore Has Definite Virtues—and Vices	14
Avoiding Exposure to Avoid Losses	15
<b>Chapter 2 How and Why Scams Survive, Thrive, and Succeed</b>	<b>17</b>
The More You Try to Scam, the Better the Odds of Succeeding	17
Persistence and Variety	18
A Successful Scam Spawns Countless Imitations	18
Old Scams Finding New Victims	19
Examples of Health Insurance Fraud	21
Simple Technology Tricks Reap Major Results	21
Trust Few, Share Little	22
A Little Knowledge Is Indeed Very Dangerous	23
Taking Advantage of Human Nature and Gullibility	23
Common Traits of Fraud Victims	24
<b>Chapter 3 Types and Methods of Attacks</b>	<b>27</b>
The Social Side of Attacks	27
You've Been Engineered ... Socially, That Is!	28
Social Engineering Tools and Tricks	28

Anatomy of a Blatant Phishing Attack	30
Examining the Source Code	31
The Technical Side of Attacks	33
Disguise and Conquer	33
Hidden and Malicious Payloads	33
The Mechanics of Drive-By Downloads	34
Information Harvesting	34
Malvertising	35
CEO Fraud	35
Webcam Hijacking	35
Other Attack Vectors	36
Cryptocurrencies	36
Example Scamming and Phishing Emails	37
<b>Chapter 4 Phishing Explored and Explained</b>	<b>45</b>
The Basic Laws of Phishing	45
Imitate	46
Motivate	46
Take Action Now!	47
Attack Anatomy 2: A Well-Done Phish	48
The First Surprise: Steganography	48
The Second Surprise: A Malicious Attachment	50
Telltale Signs in a Sophisticated Attack	52
Attack Anatomy 3: Fake File Attachment	53
URL Shortening: The Good and Bad	54
Social Engineering Red Flags	55
Surefire Ways to Avoid Phishing	57
What Criminals Want from Victims	57
How Criminals Lure Victims	58
How Criminals Profit from Data Theft	58
<b>Chapter 5 Variations on the Phishing Theme: Smishing and Vishing</b>	<b>61</b>
Anatomy of a Smishing Attack	61
Selecting the Bait	62
Setting the Hook	62
A Smishing Example	62
Anatomy of a Vishing Attack	65
Selecting the Bait	65
Setting the Hook	65
A Vishing Example	66
Why Smishing and Vishing Works	67
Other Possible Variations Surely Lie Ahead	68
Avoidance Techniques to Live By	68
<b>Chapter 6 Targeted Scams: Spear Phishing, Whaling, and More</b>	<b>71</b>
Spear Phishing Attacks	72
Whaling Attacks	73
Social Engineering Redux: Upping the Ante	74
Anatomy of a Whaling Attack	75
Spotting an Attack	77

## Table of Contents

Surefire Spear Phishing and Whaling Avoidance _____	79
CEO Fraud _____	79
<b>Chapter 7 Understanding Cybercrime Losses and Exposures _____</b>	<b>81</b>
Cybercrime Reporting and Analysis _____	81
Trends in Cybercrime _____	81
Internet Crime Statistics _____	82
Losses Due to Cybertheft _____	83
How Cybercrime Gets Monetized _____	83
A Terrible Spot for SMEs _____	84
The Patco Example _____	85
Reducing Phishing Risks _____	86
Trends and Changes That Could Alter the Cybercrime Landscape _____	88
<b>Chapter 8 Scary Reports and Statistics on Cybercrime _____</b>	<b>89</b>
Loss Reporting Trends and Information _____	90
The Many Forms of Modern Fraud _____	91
The Iceberg of Unreported Losses _____	92
Loss Reports: 2016–2019 _____	93
Reported Losses for 2019 _____	93
Reported Losses for 2018 _____	94
Reported Losses for 2017 _____	96
Loss Projections _____	98
Emerging Trends _____	99
Speculation Abounds _____	99
Gaping Security Holes Pose Big Risks _____	99
<b>Part 2 Business Use Cases: Anatomy of Various Cyberheists _____</b>	<b>101</b>
<b>Chapter 9 Bank Scams _____</b>	<b>103</b>
A Sampler of Banking Scams _____	103
Attackers Target Credit Card Processing _____	103
Hackers Use Malware to Steal from Taiwanese Bank _____	104
World’s Biggest Cyber Robbery _____	104
JP Morgan Chase Hacked _____	104
Account Information Scams _____	105
Patco Construction Company, Inc. versus People’s United Bank d/b/a Ocean Bank _____	105
Consequences to Banks and Customers Alike _____	106
SMEs Vulnerable to Banking Scams _____	106
SMEs and Banking Trojans _____	107
SMEs and Federal Investigations _____	107
Large-Scale ACH Fraud _____	107
Payroll Fraud _____	108
Understanding Scamming Mechanisms _____	108
How to Avoid Bank Scams _____	109
Training Is Key _____	109
Technical Defenses Are Important, Too _____	110
<b>Chapter 10 Credit Card and Epayment Scams _____</b>	<b>111</b>
The World of Credit Card Scams _____	111
Credit Card Fraud by Botnet _____	111

An Example of Botnet Theft _____	113
Department Store and Private Label Card Fraud _____	115
Department Store Credit Card Fraud _____	115
Gift Card Fraud _____	115
PayPal Scams _____	116
Understanding Scamming Mechanisms _____	117
How to Avoid Card and Epayment Scams _____	119
Chip and Pin Cards _____	120
<b>Chapter 11 Mortgage Rescue Scams _____</b>	<b>121</b>
A Sampler of Recent Scams _____	121
The Phantom Help Scam _____	121
The Bailout Scam _____	122
The Bait-and-Switch Scam _____	122
Mortgage Escrow Fraud _____	123
Understanding Scamming Mechanisms _____	123
Bad Advice _____	124
“Let Us Help You” _____	124
“We Can Help You Start Over” _____	124
“Stop Talking to Your Bank” _____	124
“We Can Buy and Rent It Back to You” _____	124
“We Will Cover Your Losses” _____	124
“Transfer the Money” _____	125
How to Avoid Mortgage Rescue Scams _____	125
Knowing the Vulnerabilities That Are Attractive to a Scammer _____	126
Seeking Professional Help _____	126
Understanding What to Do and What Not to Do _____	126
Wrapping Up _____	127
<b>Chapter 12 Automated Clearing House Scams _____</b>	<b>129</b>
The Most Lucrative Scam Against Organizations _____	129
How Big Is the Score? _____	130
Targeting Objectives and Requirements _____	131
An Example of a Basic ACH Scam _____	131
Scouting for the Right Spot _____	132
Casting the Lure _____	132
Jumping Ship _____	133
And Like That—Poof!—The Money Is Gone _____	133
“Mules” Willing, Waiting, and Able _____	133
Trojan Not Required _____	134
Occasional Scam Elaborations and Distractions _____	135
How Fraud Detection Plays into ACH Scams _____	135
Avoiding ACH Scams _____	136
Increasing User Awareness _____	136
Implementing Auditing and Controls _____	136
Reviewing Corporate Accounts Daily _____	137
Technology Steps That Can Help Avoid ACH Scams _____	137
Implementing Defenses _____	137
Diversifying Defenses _____	138
Minimizing the Number of Accounts and Personnel That Permit ACH Transfers _____	139

## Table of Contents

<b>Chapter 13 Retailer Scams</b>	<b>141</b>
Bigger Organizations Attract Criminal Attention	141
A Sampler of Recent Scams	142
Gift Card Scams	142
Brick-and-Mortar Store Scams	142
Web-Based Scams	143
Promotion Scams	144
Discount Scams	144
Bogus Account Credit Scams	145
How to Avoid Retailer Scams	146
Gift Card Scam Protection	147
Promotion and Discount Scam Protection	147
Bogus Account Credit Protection	148
<b>Chapter 14 Social Networking Scams</b>	<b>149</b>
What Are Social Networking and Social Media?	149
Watch for That Lure; It's Probably Obscured	150
Anatomy of a Twitter Phish	150
Paying for Services You Don't Want or Need	151
Anatomy of a Facebook Phish	152
Quizzes and Other Applications	152
Instant Messaging	153
Spamming	153
Videos on Facebook	153
Phishing and Other Social Media	153
YouTube	153
LinkedIn	154
Blogs	154
How to Avoid Phishing on Social Media	154
Twitter Precautions	155
Facebook Precautions	155
LinkedIn Precautions	156
Blog Precautions	156
<b>Chapter 15 Ransomware</b>	<b>157</b>
History of Ransomware	157
Ransomware Basics	159
Traditional Ransomware	161
Ransomware 2.0	164
More Malicious Ransomware	164
The Future of Ransomware	166
Defenses	166
Recognize the Problem	167
Preventive Controls	167
Early Warning Detection	167
Communications	168
<b>Chapter 16 Mobile Threats</b>	<b>169</b>
Lack of Login	169
Malicious Public Hotspots	170

Malicious Applications _____	170
Phishing _____	171
Spyware _____	172
Data Leakage _____	172
Lost Phone or Device _____	172
Keep Your Mobile Device Updated _____	173
<b>Chapter 17 Nation State Threats _____</b>	<b>175</b>
The Role of the Nation State _____	175
Zero-Day Vulnerabilities _____	176
Legalities _____	177
Military Uses for Cyberwarfare _____	177
Snowden _____	178
North Korea Sony Pictures Attack _____	179
Infrastructure Threats _____	179
Chinese Advanced Persistent Threat _____	179
Stuxnet and Other Attacks _____	180
Foreign Election Interference _____	181
Threats to Businesses _____	181
What Can Be Done? _____	182
<b>Part 3 Countering Cybercrime _____</b>	<b>183</b>
<b>Chapter 18 Fundamentals of Safe Computing _____</b>	<b>185</b>
What Does Safe Computing Mean? _____	185
Best Practices for Safe Computing _____	185
Physical Security _____	186
Passwords _____	187
Using Secure Passwords _____	188
Social Engineering and Phishing _____	189
Should I or Shouldn't I? _____	190
Look for TLS to Keep You Safe _____	190
Network Security _____	193
Public Use of Private or Public PCs _____	194
Antimalware _____	195
Safe Internet Use _____	196
Watch What You Download _____	196
Don't Click Any Ol' Link _____	196
Verify the URL Domain _____	196
<b>Chapter 19 Syncing Up Security Policies, User Training, and Monitoring _____</b>	<b>199</b>
Security Policies _____	199
Why Security Policies Vary _____	199
Creating and Enforcing Security Policies _____	200
Adaptability Is Key _____	200
Parts That Make the Whole _____	200
An Example of a Security Policy Outline _____	201
A Closer Look at Acceptable Use Policies _____	202
What's in an AUP? _____	203
User Training _____	204



## Table of Contents

Break Out the Surveys _____	205
Monitoring Techniques _____	205
Tracking User Activity and Behavior _____	206
<b>Chapter 20 Protecting People and Assets with Security Technology _____</b>	<b>209</b>
Information Security Principles and Practices _____	209
Access Controls _____	210
Overview of Permissions and Access Controls _____	210
Restricting Electronic Access _____	212
Minimizing Use of Elevated Privileges _____	212
Restricting Physical Access _____	212
Clear-Cut Security Classifications _____	213
Separation of Duties _____	214
Regular Security Policy Audits, Updates, and Remediation _____	214
Using Security Technology _____	215
Client-Side and Server-Side Security Considerations _____	215
Securing the Networking Infrastructure _____	216
Covering All the Access Points, Starting at the Perimeter _____	216
Controlling Remote Access _____	218
Establishing Malware-Free Conditions Throughout a Network _____	220
Implementing Network Access Control and Management _____	220
Applying Patches and Security Updates _____	221
<b>Chapter 21 Managing Online Security Issues _____</b>	<b>223</b>
Defense in Depth _____	224
Policies _____	224
Firewalls _____	225
Patching _____	226
Password Vaults _____	226
Antimalware Applications _____	227
Anti-Phishing Systems _____	227
Anti-Phishing in Web Browsers _____	228
Online Reputation _____	229
User Education and Awareness _____	229
<b>Chapter 22 Cyber Insurance _____</b>	<b>231</b>
What is Cyber Insurance _____	231
Cyber Insurance Statistics _____	232
How is the Price Determined? _____	233
What to Do When There Is an Incident _____	233
Questions to Ask About Cyber Insurance _____	234
What is covered under a cyber insurance policy? _____	235
Is the policy an extension to an existing policy or does it standalone? _____	235
Are there any deductibles or coinsurance amounts? _____	235
Does the policy exclude for criminal or intentional acts? _____	236
What is the liability coverage for third parties? _____	236
Is social engineering covered? _____	236
Are phishing and spear phishing covered? _____	236
What is the coverage for forensic investigations? _____	237
How does the policy handle a breach that is result of negligence rather than maliciousness? _____	237

What are the limits for payouts for each type of coverage? _____	237
Does it cover cyberwarfare events? _____	237
<b>Chapter 23 Fostering Security Awareness _____</b>	<b>239</b>
What Is Security Awareness? _____	239
About Security Awareness Training (SAT) _____	240
Benefits of Online SAT _____	242
Typical SAT Course Topics _____	242
KnowBe4 Security Awareness Training _____	243
Courseware _____	244
Reporting _____	245
Pricing _____	245
Phish Alert Button _____	245
KnowBe4 Simulated Phishing Security Tests _____	245
Consulting Services _____	246
<b>Appendix A Acronyms and Glossary _____</b>	<b>249</b>
List of Acronyms _____	249
Glossary _____	253
<b>Appendix B Resources _____</b>	<b>263</b>
Banking Security _____	263
Credit Card Security _____	263
General Scam/Fraud Information and Security _____	264
Government Agencies _____	265
Protection Software and Utilities _____	266
Who to Contact/Where to Complain _____	267
<b>Appendix C References _____</b>	<b>269</b>
<b>Index _____</b>	<b>277</b>

## List of Tables

Table 1: Top 10 Internet User Populations, by Language.....	3
Table 2: IC3 Complaints Received 2009–2019.....	5
Table 3 Attack Lures Versus Legitimate Interactions.....	78
Table 4 Going Rates for Stolen Cyber Info.....	83
Table 5 Some Notable Events in the History of Ransomware .....	157



# List of Figures

Figure 1 Example malware exploitation life cycle .....	8
Figure 2 Snippet from a Hypertext Markup Language (HTML) phishing message .....	30
Figure 3 A snippet from the message header shows that something is up! .....	31
Figure 4 These Message-ID, Reply-To, and From addresses are carefully faked .....	32
Figure 5 The spam-filtering service detects that this message is a forgery .....	32
Figure 6 Sample Phishing Email .....	37
Figure 7 Phishing Email .....	38
Figure 8 Phishing Email .....	39
Figure 9 Advanced-Fee Scam .....	39
Figure 10 COVID-19 Scam .....	40
Figure 11 Phishing Scam .....	40
Figure 12 Typical Advanced-Fee Scam.....	41
Figure 13 Charity Scam .....	42
Figure 14 Typical phishing email.....	46
Figure 15 The message itself is only an image, but it contains two surprises.....	49
Figure 16 Outlook shows that this message comes with an attached ZIP file .....	51
Figure 17 Part of the message header of the FDIC phishing email.....	52
Figure 18 Fake file attachment image phish example .....	53
Figure 19 Previewing a shortened URL in Firefox.....	54
Figure 20 TinyURL indicates that the shortened URL is linked to the KnowBe4 website .....	55
Figure 21 Social Engineering Red Flags.....	56
Figure 22 Example smishing attempt .....	63
Figure 23 A blatant smishing attempt aimed at hooking people with debt problems .....	64
Figure 24 This mocked-up text from the whaling message described in this chapter looks somewhat like a real subpoena .....	76
Figure 25 A portion of a PDF of a subpoena downloaded from the U.S. Courts website .....	77
Figure 26 Annual number of complaints and losses received by the IC3, 2015 to 2019 .....	82
Figure 27 Fraud by Victim Count for 2019.....	93
Figure 28 Fraud by Victim Loss for 2019.....	94
Figure 29 Fraud by Victim Count for 2018.....	95
Figure 30 Fraud by Victim Loss for 2018.....	96
Figure 31 Fraud by Victim Count for 2017 .....	97
Figure 32 Fraud by Victim Loss for 2017.....	98
Figure 33 A typical botnet usually includes thousands or hundreds of thousands of computers .....	113

Figure 34 A simplified example of using a botnet to commit credit card fraud.....	114
Figure 35 Location of bank's routing number and account holders bank account number on a typical U.S. check .....	130
Figure 36 An ACH scam in action .....	132
Figure 37 One email that offers discounted office supplies .....	145
Figure 38 A second email offering discounted office supplies .....	145
Figure 39 The real Twitter home page shows twitter.com in the address field of a web browser .....	151
Figure 40 Which ransomware variants raised the most money?.....	159
Figure 41 Example ransomware message .....	162
Figure 42 Example ransomware message .....	163
Figure 43 Real World Example of Threatening Everyone .....	166
Figure 44 An example of a fictitious phishing email .....	189
Figure 45 Lock in Google Chrome (top), Microsoft Edge (Middle), and Firefox (top) (bottom)	191
Figure 46 Clicking on the lock symbol to find out about site security.....	192
Figure 47 Insecure site indicator.....	192
Figure 48 Turning off network options on Windows 10.....	195
Figure 49 The NTFS permissions tab for a folder.....	211
Figure 50 Protecting the network perimeter with a firewall.....	217
Figure 51 An IDS and web proxy server create a stronger perimeter .....	218
Figure 52 A VPN is an encrypted communication tunnel across the internet .....	219
Figure 53 KnowBe4 delivers comprehensive security awareness training .....	243
Figure 54 The SAT modules are user friendly and engaging .....	244

# Preface

The book you're holding, or viewing on a screen, is meant to educate you about the dangers of conducting business online. In particular, it covers several forms of **phishing**, a type of **social engineering** attack delivered using technology such as the internet and phones.

Our goal is to help you recognize the increasing danger that individuals and organizations face when they use the internet and other technologies, especially when conducting financial activity, and take proactive measures to protect your organization. These risks include theft of sensitive information, theft of goods and services, loss of intellectual property, the inability to use equipment and assets, and exposure to fraudulent online money transfers that empty your bank accounts: a **cyberheist**.

The dangers are real, and widespread. In the United States, losses to internet crime exceeded \$3.5 billion in 2019, and these figures are going up. Small to medium enterprises are particularly vulnerable to fraudulent wire transfers by organized cybercriminals. These crooks have become very skilled at social engineering and getting your organization's online banking credentials.

In addition, regulated organizations that handle private customer data must be even more vigilant. They face stiff legal and financial penalties if a thief breaches the data they store and manage. The fallout can cost an organization anywhere from thousands to millions of dollars, ruin its reputation, and possibly shut it down.

Don't become a statistic. Read this book and apply the strategies and techniques described within to protect your organization from a potentially devastating cyberheist.

## *About This Book*

This book consists of 23 chapters, divided into four parts.

Part 1, "The Business of Cybercrime," includes Chapter 1 through Chapter 8. In the early chapters, you learn about cybercrime attacks and techniques, and what drives attackers to create more and better scams. You also learn about phishing and ransomware, and several interesting variations on that theme. Part 1 continues with an analysis of how cybercrooks target certain victims (Chapter 6), and an overview of cybercrime losses and exposures (Chapter 7). It concludes with a detailed look at the percentages of cybercrime incidents in "Scary Reports and Statistics on Cybercrime" (Chapter 8).

Part 2 is entitled “Business Use Cases: Anatomy of Various Cyberheists” (Chapter 9 through Chapter 17). Each chapter tackles scams targeted toward a certain industry: banking, credit card and epayment processing, mortgages, banking clearinghouses, retail sales, and **social networking**. The chapters also explore scam scripts, attack methods, and protective strategies.

Part 3 of this book is called “Countering Cybercrime” (Chapter 18 through Chapter 23). It describes the fundamentals of safe computing (Chapter 18); how to integrate security policy, user training, and monitoring (Chapter 19); and how to protect people and assets with security technology (Chapter 20). You learn about online banking vulnerabilities in detail, and how to avoid them, in Chapter 21. Cyber insurance is discussed in Chapter 22. Part 3 concludes with a discussion of how to raise security awareness at work and introduces the KnowBe4 training program (Chapter 23).

You can also find a list of acronyms and a glossary in Appendix A, resources in Appendix B, and references in Appendix C.

*We use specific social networking companies such as Twitter and Facebook in examples in this book. Our intent is not to disparage these well-respected companies. Rather, we seek to point out the dangers that cybercriminals pose on these highly popular sites.*

## Special Elements Used in This Book

Throughout this book, you’ll see a bomb icon here and there, and other text set off by bounding lines, italics, or shading. These are used to flag specific types of information and content. Here’s a brief key to what you’ll find:

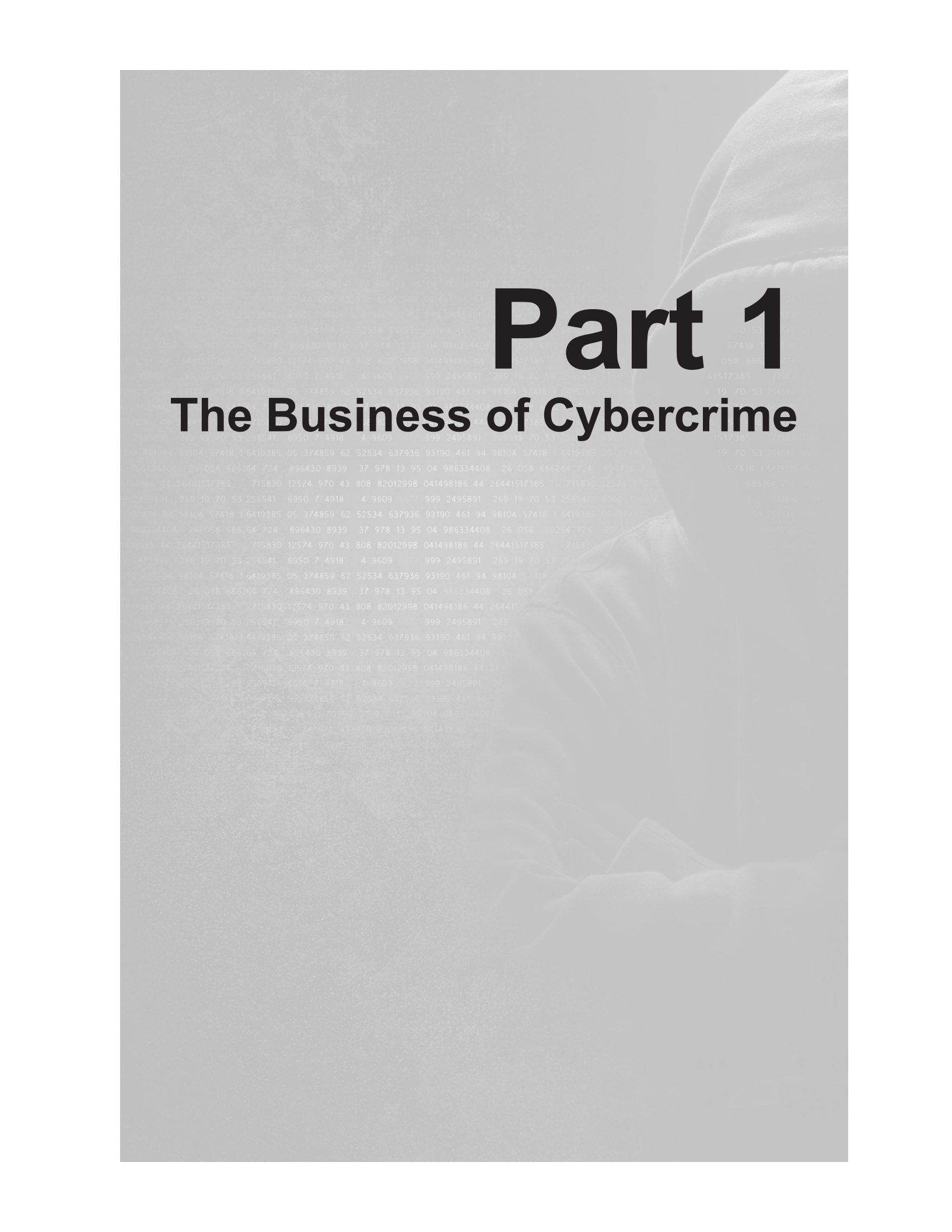
- Notes: Additional technical or background information to help you understand attack techniques, internet technology, or security tools and methods
- Warnings: Cautions about things to watch out for, avoid, or notice when working online
- Cyberalerts: Flagged with a bomb icon, this is information about cybercrime terms, tools, techniques, and methods; often, definitions for specific types of cybercrime attacks



## Contact Us

We’d like to hear from you with your comments, criticisms, and questions about this book. Please visit our website at [www.KnowBe4.com](http://www.KnowBe4.com) or email us at [cyberheist@knowbe4.com](mailto:cyberheist@knowbe4.com).





# Part 1

## The Business of Cybercrime



# Chapter 1

## What Drives Cybercrime?

Willie Sutton was a famous twentieth-century bank robber falsely credited with answering the question “Why do you rob banks?” with “Because that’s where the money is.” This saying is so well known, it’s sometimes called “Sutton’s Law.” While Mr. Sutton never actually said this, it does explain the basic driver for **cybercrime**. An enormous number of people are active online, and thieves therefore turn to the internet to find victims.

How many people are active online? Table 1 shows estimates for the global online population, by language, for the first quarter of 2020.

***Table 1: Top 10 Internet User Populations, by Language***

Position	Language	Internet Users
1	English	1,186,451,052
2	Chinese	888,453,068
3	Spanish	363,684,593
4	Arabic	237,418,349
5	Portuguese	171,750,818
6	Indonesian / Malaysian	198,029,815
7	French	151,733,611
8	Japanese	118,626,672
9	Russian	116,353,942
10	German	92,525,427

Source: [Internet Usage by Language: Top 10 Languages](#) [1]

The total for all these populations exceeds 3.525 billion users! However, Table 1 lists only the top 10 language populations on the internet, so the total internet population must be even bigger. It would probably be safe to add another 1 billion internet users to the preceding total for a rough guesstimate of 4.5 billion internet users worldwide. Given a global population of 7.8 billion in 2020, that means more than 2 in 3 people on the planet use the internet.

That’s a huge pool of potential victims by any standard. All these users could be accessible to thieves using any working internet connection. Because so many people who use the internet

## Chapter 1

### What Drives Cybercrime?

also use credit cards, do their banking, and manage financial accounts online, it's no wonder that cybercrime is prevalent. It's also no mystery that cybercrime rates are going nowhere but up.

## *What Exactly Is Cybercrime?*

One simple definition of **cybercrime**, or **cyberheist**, is “a crime whose commission involves a computer, smartphone, or other so-called smart devices.” A better definition for this book could be “a crime committed using an internet-connected computer or device.” This broad definition includes any kind of wrongdoing that involves interacting on the internet. Thus, it covers massive email broadcasts (spam) that involve no other overt criminal activity. It also covers online postings involving libel, defamation, or hate speech, all of which are regarded as criminal in some jurisdictions.

The cybercrimes that are the focus of this book must be defined more narrowly. We want to dig deeply into various forms of criminal activity that targets phones, computers, and computing resources. We are especially interested in attempts to acquire and misuse sensitive information, primarily to rack up ill-gotten gains. This means analyzing attacks or scams of many kinds. Some seek to obtain accounts and passwords for websites. Others attempt to gain access to people's online banking or financial services. Some involve theft of securities or commodities. Some seek to misuse credit cards without notification or permission. Some hold the data on computers for ransom. Ultimately, the cybercrimes that interest us most are those that supposedly also excited Mr. Sutton's interest in banks: These cybercrimes go after other people's money.

Some of these cybercrimes are the result of cyberterrorism, cyberwarfare or cyberespionage, which are groups, sometimes sponsored by governments, who have a specific political or war fighting agenda for their malicious activities. The result to corporations is the same – theft of computer resources and finances.

There's plenty of evidence that cybercrime occurs frequently, no matter how you measure such things. The [Internet Crime Complaint Center](#) (IC3) is a joint partnership between the U.S. Federal Bureau of Investigation (FBI) and the [National White Collar Crime Center](#) (NW3C). The IC3 receives cybercrime complaints and reports statistics, acting as a central referral system for law enforcement and regulatory agencies. Table 2 provides information on complaints of cybercrime that the IC3 received from 2009 through 2019.

**Table 2: IC3 Complaints Received 2009–2019**

Year	Number of Complaints Received	Losses (in millions or billions)
2019	467,361	\$3.5 B
2018	351,937	\$2.7 B
2017	301,580	\$1.4 B
2016	298,728	\$1.5 B
2015	288,012	\$1.1 B
2014	269,422	\$800.49 M
2013	262,813	\$781.84 M
2012	289,974	\$525.44 M
2011	314,246	\$485.25 M
2010	303,809	Not available
2009	336,655	\$559.70 M

Source: [FBI's IC3 2019 Internet Crime Report](#) [2]

As you can see from Table 2, hundreds of thousands of cybercrimes are committed annually and the dollar volume of losses is increasing. The table only shows those crimes submitted to IC3. It can be safely assumed that the global statistics are several times larger. Today, headlines regularly report enormous losses due to cybercrime. It's not unusual to read about millions of dollars being lost in a single heist.

In this book, we explore an interesting and disturbing trend: Businesses are bearing an ever-increasing portion of the impact of cybercrime. At the same time, large numbers of individuals are experiencing identity theft and related financial losses and ruined credit ratings.

## *Who's a Target for Cybercrime?*

Individuals, businesses, and governments are targets for cybercrime. With more people targeted at work, individuals who fall prey to cybercrime force their employers to suffer and absorb related losses. The answer to the question "Who's a target for cybercrime?" is "Anybody with an email inbox, who surfs the web, or who has a computer, a smartphone, or any so-called smart device (referred to as the Internet of Things or IoT). "That's nearly everybody who uses the internet, which is more than 4.5 billion people, every business, every government, and every smart device.

Let's look at an example. An accounting clerk named Sally Smith types the URL of her bank's website into the browser, just like she does every day. Suddenly, a pop-up appears on her screen,

## Chapter 1

### What Drives Cybercrime?

with a very scary message saying her computer has been infected by 876 viruses. All is not lost, however! The screen tells her to click a button to download some “cleaning” software that will kill all the nasty viruses automatically for her. She’s relieved for the help and clicks the button. A few minutes later, another pop-up appears. This time it demands \$500 in bitcoin within 36 hours or her data will be lost forever! Nothing on her computer works anymore.



#### Ransomware

**Ransomware** is exactly what it sounds like – computers, data, and other sensitive information (like passwords) are taken hostage by malicious software and gangs and is held for ransom. Traditional ransomware encrypted the data and asked for a ransom to decrypt it. Ransomware has evolved into also copying the data and other sensitive information and asking for a ransom to be paid so that the hackers don’t reveal the stolen, confidential data publicly on the internet or to other hackers.

Ransomware has the following characteristics:

- ✓ It usually gains initial access to a computer or network using social engineering, unpatched software, or password guessing.
- ✓ The ransomware program “dials home” to update itself and to notify its owner of its new conquest.
- ✓ The ransomware may look for and spread to other computers within its host environment, looking for and logging every password it can find along the way.
- ✓ The ransomware gang owners will often investigate the new victim, looking to calculate how much ransom they should charge and what information should be stolen and encrypted.
- ✓ The malware or gang will often look for the most valuable “crown jewels” of the network and copy it to another location under the hacker’s control.
- ✓ After the ransomware malware or gang has gained maximum exploitation pressure, it will execute its payload, encrypting all the involved computers and notify the affected users with a message on their screen.
- ✓ The ransomware program will tell the victims what has happened (i.e., data stolen and encrypted) and ask for payment using a cryptocurrency.
- ✓ The ransomware program or gang may also publicly blog the takedown, notifying the public, employees, and customers of the data compromise and their demands.
- ✓ If the victim pays the ransom, the ransomware gang will usually send the decryption keys and not release any stolen data. The victim still often has days to weeks of

recovery time even after receiving the key, plus the effort needed to prevent future ransomware attacks from being successful.

Next, consider a common phishing attack that targets financial professionals at small to medium enterprises (SMEs) (see Figure 1). An email arrives in Joe Biggs's inbox at example.com. It appears to originate from an **Automated Clearing House** (ACH) that processes payments for Mr. Biggs's employer. This message informs him that a payment problem is pending, and that processing has been discontinued. Feeling some concern, Mr. Biggs reads further. Next, he learns that he must provide information about his company's account in order for processing to resume. He is asked to click a handy link in the message to provide that information ASAP, so that business can get back to normal. Sounds pretty routine, doesn't it? It's not.



### Phishing

Phishing takes its inspiration from catching fish. Just as an angler uses a lure to entice fish to bite his hook, cybercriminals use hyperlinks to draw unsuspecting users to malicious websites. Phishing shares these things in common with its watery inspiration:

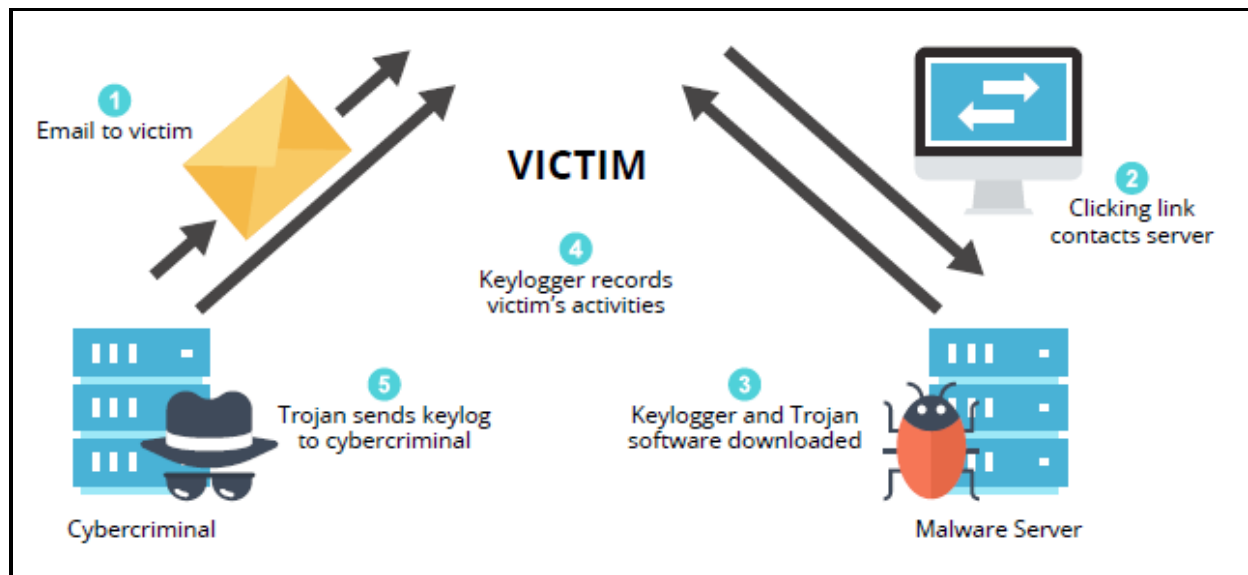
- ✓ It looks like an innocuous or even a legitimate email message, Tweet, or Facebook post.
- ✓ It seeks to get readers to provide information by responding to the message or clicking an embedded link.
- ✓ It often requests sensitive information about accounts, passwords, or identity.
- ✓ The hook gets "set" when a reader responds, even if only by clicking a link.

Security experts often label phishing as a kind of "social engineering." This term describes various techniques used to persuade users to part with information about themselves, credit card or bank information, and so forth. The idea is to glean something of value or an action to enable theft or cybercrime. No night crawlers and lures are involved, but the victims often wind up gutted anyway.

These crimes do not always involve stealing. For example, one form called a **denial of service** attack is intended to cause interruption. These may be done by a **hacktivist** (a hacker who is also an activist). They do not ask for or take money, since their intent is to promote their social or political agenda.

## Chapter 1

### What Drives Cybercrime?



*Figure 1 Example malware exploitation life cycle*

If Mr. Biggs clicks that link, he is already at risk, even if he provides no information to the web page where that link takes him. That's because simply visiting a phishing page can expose a PC to malicious software downloads. They can occur in the background, covertly, without the user's knowledge or consent.

Cybercriminals who run phishing scams are especially fond of software packages like Tox (to create ransomware) and Cobian RAT [3], which includes a keystroke logger (also called a **keylogger**) with other tools such as a camera hijacker, a voice recorder, and a command and control system.

- ✓ A keylogger is a trojan program which harvests valuable information from an unwitting PC user by recording their keystrokes and sending the information to a hacker. A keylogger records every keystroke that Mr. Biggs makes on his PC, and the **Trojan** periodically opens a backdoor to upload that keystroke log. The cyberthieves who planted this malware on his machine will comb that file carefully. They'll grab every account and password combination it contains, along with any sensitive data it might contain. If the bad guys can sniff out an online banking site and use Mr. Biggs's credentials to log in, they can transfer funds to other accounts right away. Talk about an unfortunate downside of 24/7 online banking services!
- ✓ A camera hijacker lets the hackers spy on you using your camera.
- ✓ A voice recorder records everything from your microphone and sends it to the hacker.
- ✓ Command and control let the hacker remotely control every action on your computer, including giving them the ability to download and install new software and hacker tools.



## Harvesting and Malware



To **harvest** information means to acquire data illicitly. The data is usually some form of credentials, such as account names or numbers, passwords, and **challenge-response sequences**. An unauthorized third party—usually, a cyberthief—often uses the information to impersonate the individual or organization whose credentials have been stolen.

**Malware** is short for malicious software. Malware is any software that's installed on a computer with the intention of executing malicious code and/or causing damage. Typically, the software installs without the owner's permission.

If Mr. Biggs provides the information requested on the phishing web page, the thieves don't need to bother with a keylogger, Trojan or other software. They can simply try out the information he provided and see what it gets them.

"But wait!" you're probably thinking, "Does anybody really fall for this kind of thing?" A surprising number of people do fall for such scams. In fact, according to a Google study in 2014, even poorly made phishing sites are successful at gaining people's information 14% of the time, while well-made ones work as much as 45% of the time [4].

*KnowBe4.com has run surveys at various types of firms and observed average success rates of 37.9% for its own initial simulated phishing attacks.*

## A Million Stories for a Million Scams

Let's look at a quick sampling of warnings and reports of scams from the IC3 website:

- ✓ **Emails containing malware sent to businesses concerning their online job postings:** Companies download resumes and then become infected by malware payloads. The malware harvests sensitive data for transmission to cyberheisters. This is surely a sinister way to fight unemployment!
- ✓ **Fraudulent ACH transfers connected to malware and work-at-home scams:** Infected email attachments or **drive-by downloads** on malicious web pages harvest corporate banking credentials. This enables cybercrooks to access bank accounts and make fraudulent funds transfers. People seeking to generate income while working at home fall prey to account harvesting that costs them money instead.
- ✓ **Pop-up advertisements offering antivirus software:** Users respond to bogus virus discovery and repair offers to help them get rid of viruses they don't really have. These users waste money on worthless software, and their machines fall prey to malware that can harvest sensitive data and cost them even more of their money. This software is called **rogueware**.

## Chapter 1

### What Drives Cybercrime?

- ✓ **Fraudulent email claiming to be from the Department of Homeland Security and the FBI Counterterrorism Division:** Readers who download a purported speech by Osama Bin Laden get malware instead. Thieves can then harvest and download sensitive data. Instead of keeping up with terrorism, readers get ripped off.
- ✓ **ISIS celebration in Paris with video:** Click on the links in a video of ISIS celebrating the attacks and your information may be harvested or malware installed on your computer.
- ✓ **Debt elimination schemes that offer to reduce or get rid of debt for a small fee, typically \$1,500 to \$2,000:** The scammers additionally request the entire financial history of a user, so not only are they out the money, but they are also prime targets for identity theft and credit card fraud.

This list gives a good taste of the ingenuity and resourcefulness that cybercriminals bring to online scams.



#### Drive-By Downloads

A drive-by download is a transfer of software from a web server to an unsuspecting user's computer. Normally, it requires that the victim's device have an unpatched version of a specifically targeted application. If the unpatched software can be exploited, the drive-by download occurs in the background, with no notification, when a user visits a particular web page. It's called a "drive-by" download because a user need only access the page with a vulnerable device to be subject to the download. Such downloads can install themselves on the systems on which they take up residence, which means attackers can put specific types of malware of their choosing on victims machines.

What kind of malware is in a typical drive-by download? Four categories are common. The first is a class of software called Trojans, short for Trojan horses (after the famous ruse Greek warriors used to access the fortified city of Troy in The Aeneid). After a Trojan accesses a machine on the internet, it is able to do nearly anything on it. For example, it can ship a log of keystrokes to some recipient address or give the hacker access to the camera. In the log, they're looking for accounts, passwords, and other information they can use to impersonate authorized users and steal their money. The second is ransomware, discussed on page 6. The third is called a keylogger, which records every keypress a user makes on his or her machine into a special file called a keystroke log and the fourth is a **dropper**, that lets the hacker download other malware to your computer.

Other phishing attacks recently reported from various sources include the following:

- ✓ **Attempts to collect bogus payday loans:** Disturbingly, these attacks feature lots of sensitive data about potential victims, including social security numbers, addresses, bank accounts, credit card balances, work history, and more.
- ✓ **Foreclosure-related scams:** Thieves use these scams to trick people in danger of losing their homes to waste their money on false remedies for their troubles.
- ✓ **Email account renewal scams:** These scams ask for credit card and other account information to cover a purported but nonexistent annual renewal fee.
- ✓ **Bank account and credit card information request scams:** Countless scams ask users to provide account details for hundreds of reasons, ranging from “database problems” to totally fabricated “security checks.”
- ✓ **Holding computer systems for ransom:** Malicious software locks all files on a computer so they cannot be accessed – frequently encrypting all the data – then demands a payment to return control.

For every online account access or transaction where money changes hands, there’s at least one scam that seeks to divert some of those funds into the wrong hands. For really popular forms of online financial activity, there are bound to be scads of such scams.

## *A Case of Criminal Culture*

Criminals often learn their craft from other criminals, sometimes through direct contact and outright mentoring and sometimes through observation of what kind of crimes prove most successful. Cybercrime is a booming growth industry because it combines many characteristics that are especially appealing to criminals, including the following:

- ✓ **No physical risk:** Crime can be a dangerous business, particularly mugging and other forms of armed robbery. Cybercrime involves no direct contact with victims and hence poses no physical danger to its perpetrators.
- ✓ **No need for proximity:** Criminals must interact with their victims to commit their crimes. Working through the internet lets criminals interact with potential victims from anywhere in the world, with no real-world contact needed, in a way that virtually guarantees preserving their anonymity.
- ✓ **A work-when-you-want schedule:** Sending email and putting up web pages require no real-time interaction with victims. A victim chooses to read an email or visit a web page whenever he or she wishes. The criminal only needs to check for resulting information harvests and be ready to act fast once potentially valuable information is available.
- ✓ **Tremendous opportunity:** The sheer size of the internet user community lets criminals’ experiment with scams. They know they need to score with only a small

## Chapter 1

### What Drives Cybercrime?

- number of emails or clicks to reap sometimes significant gains. It's easy to generate tens of thousands to millions of email messages, and it's also easy to post tweets or Facebook pages to large audiences. Cybercriminals try all kinds of tricks to draw users to their malicious websites.
- ✓ **Small effort and big rewards:** Until the internet came along, scamming required significant effort and finesse to generate earnings. It also involved physical risk and being in close proximity to victims. Modern criminals only need to invest small amounts of time and effort to run internet scams, but they can easily reap thousands of dollars in return.
  - ✓ **Lack of legal jurisdiction.** Scammers live and operate in countries throughout the world. Even finding the scammers can be virtually impossible, and if they are located, the investigators are often frustrated due to lack of legal jurisdiction, extradition, and even lack of laws about the scammer's activities.

Cybercrime is easy to do, involves little or no risk for criminals, and lets them work when and how they want, from any location in the world. If this sounds like an ideal job to you, think how it sounds to those with few scruples and a desire to make a quick-and-dirty buck.

## Cybercrime Learning and Lore

There's more to cybercrime than ease, low risk, convenience, and payoffs. There's a learning curve to climb, and there's also a need to master the tools of the trade. Lots of successful scams breed imitation. Once a cybercrook learns how to run a scam, performing variations or refining targets involve little additional effort. Crooks can watch and learn easily from more experienced ones. After that, they can quickly get scams of their own going, too.

You already read about the Cobian RAT toolkit, which combines a keylogger and a Trojan to make it easy to obtain and harvest accounts, passwords, and other sensitive information from unwary users. Cobian RAT is one of many popular toolkits that cybercriminals can use to package malware downloads that "phone home" to report on the user data they gather. For someone motivated by the illicit returns these tools can generate, spending a few days learning to use them is a modest investment for the "pot of gold" at the end of the road.

By watching others launch and manage scams, cybercriminals quickly learn how to scam. They formulate their own scam scripts, distribute emails (or Twitter feeds), and post web pages. Then they sit back and wait for results so they can take further action. This further action is likely to involve separating victims from their funds via unauthorized funds transfers, illicit credit card outlays, crooked epayment collections, and other methods of accessing account balances.

*It takes only one or two trips around the block with a more experienced cybercrook for trainees to catch on and then start running scams for themselves.*

## *Variations on a Scamming Theme*

So far, we've explored a basic and simple scam: Create an email to provoke user action, harvest access information in response, and use that information to steal from victims. This takes little computing sophistication and is simple to implement. A scam appeal—be it email, Twitter feed, Facebook page, or whatever—is broadcast to as many addresses as possible, and cybercrooks sit back and wait for a response.

There are also elaborations on this scheme. In keeping with complex scams from the pre-internet era, cyberthieves may research a specific group of victims. Then, they tailor a scam that's focused on and effective for a narrower audience. Thus, for example, ACH scams target financial or accounting professionals at SMEs. There's work involved in putting together a hit list, but professional association membership lists and websites, and even online phonebooks, make it easy to identify such people. These folks are most likely to handle electronic banking for companies where they work. Thus, they're most likely to have (or provide) the account information and passwords cyberthieves need to hijack those accounts and redirect funds as they please.

Even more sophisticated scams have been documented. After a particularly successful account harvest, a group of cyberthieves ran several electronic funds transfers against a victim company's accounts. At the same time, another group mounted a denial of service attack against the target company. The attack prevented the company's servers from accessing the internet until after the first group transferred the ill-gotten funds. Because of the delay, automatic notifications didn't reach the intended recipients until it was too late to disallow those transfers.



### **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks**

On the internet, a **denial of service** (DoS) (one system attacking another) and **Distributed Denial of Services** (DoS from many systems) attacks take servers or networks out of play. Basically, such attacks involve overwhelming specific servers with so much traffic that they can't do their normal jobs. If a server is totally busy dealing with such an attack, it doesn't have the resources to do anything else. In the DoS attack just mentioned above, cyberthieves drowned the servers with huge volumes of bogus network traffic. Those servers would normally issue fraud alerts to account holders and security personnel. All the bogus traffic bogged down the servers, preventing them from sending those alerts to the right people. In turn, this allowed other thieves to complete a series of funds transfers and siphon money out of the company's bank accounts.

## *Internet, and the Money Is Easy*

By law, credit cards are protected from fraudulent charges made over the phone or online; liability is limited to \$50 of the purchase (usually waived by banks) for physically made purchases. Banks generally also provide similar protections for debit cards, and according to the Electronic Funds Transfer Act, consumers are not liable for fraudulent electronic transactions. However, we recommend not paying with debit cards. Federal regulations are different for businesses and many banks exclude purchases made on commercial cards from their liability protection and may also exclude small business cards in the same way.

EFT regulations state that if the consumer notifies the bank within two business days, they are only liable for the first \$50 (often waived by the bank). The liability goes up to \$500 if the consumer notification takes longer than 2 days. If the consumer doesn't notify within 60 days, they are liable for the full amount. [5]

*A surprising number of SMEs, including school boards, municipal authorities, fire and police departments, and so forth, do not purchase cybersecurity Insurance. Any organization without such coverage is responsible for losses if they fall victim to online fraud.*

Once a cyberthief gains access to an online bank account, he or she often changes the account settings to enable money transfers to other accounts. Favored techniques here include authorizing electronic funds transfers (EFTs) where such transfers are not already authorized. Sometimes a cyberthief authorizes international funds transfers when existing account settings may only permit funds to be transferred to other U.S. banks.

*Favorite offshore transfer destinations for cyberthieves include Bulgaria, Romania, the Ukraine, the Baltic Republics, Russia, and Nigeria, among others.*

Sometimes, cybercrooks transfer money multiple times, in an effort to obfuscate the wire trail from the source to the ultimate destination. In such cases, the crooks may open temporary accounts just to receive stolen funds. Someone will close those accounts once the funds move closer to their ultimate recipients. Occasionally, cybercrooks recruit local confederates (known as mules) to set up accounts and receive and forward stolen funds. This further obscures the money trail that EFTs leave behind. Funds transfers may involve intermediate hops in countries with lenient banking laws and where depositor anonymity is favored over criminal prosecution and restitution of illicit gains.

## *Offshore Has Definite Virtues—and Vices*

Many cyberthieves set up operations in countries, often Eastern European, where law enforcement for cybercrime is lax, lackadaisical, or simply absent. Some countries choose not to

prosecute such acts. Their leaders perceive no “local harm” involved for operations that funnel hard currency inside their borders because a ready and steady cash flow can provide many fiscal benefits. Other countries may be subject to graft and corruption. They offer a safe haven to cybercriminals, as long as local authorities and power brokers get a “fair share” of the proceeds.

The internet is mostly insensitive to location and geography. This makes committing cybercrime possible and often absurdly easy. Criminals just set up shop where their offenses are ignored, tolerated, or treated as a source of income. This also makes it difficult for law enforcement in the United States, the European Union, and other areas to track down and prosecute perpetrators. Even in these circumstances, the FBI and other law enforcement bodies sometimes mount long-term, sophisticated “sting-and grab” operations. They snare and then capture particularly glaring offenders and try them in U.S. courts. Once cybercriminals get into that system, things usually turn out much less favorably for those found guilty.

## *Avoiding Exposure to Avoid Losses*

The old saying goes, “An ounce of prevention is worth a pound of cure.” Where cybercrime is concerned, users who avoid clicking email, Twitter, or Facebook links avoid the possibility of exploiting their systems with malware. In turn, they skip the part where their accounts and passwords get harvested. That prevents cyberthieves from using their information to steal, either from individuals or business concerns.

The motto at KnowBe4.com is “stop, look, and think before you click.” Savvy readers should internalize this motto for themselves as “I think before I click.” If you don’t click on a questionable link, you substantially reduce the opportunity for a scam to succeed. Nor is there any way for cyberthieves to get their hands on your system or to harvest your accounts, passwords, and other sensitive data.

To be clear, many types of attacks don’t require clicking links. The vast majority of DDoS attacks don’t involve human interaction at all. Hackers frequently break in through unpatched software on servers, SQL injection exploits, and so on. Thus, while the act of clicking links is involved in most cybercrimes, that’s not the whole story. However, that being said, you can significantly improve your odds by practicing “stop, look, and think before you click.”

\*\*\*

Cybercriminals work every minute of every day coming up with new attacks and new ways to break into business, personal, and government computer systems from the internet. You must spend the time to understand how they can attack, their objectives, and how you can defend yourself. Otherwise, you could be responding to breaches that cause significant damage to your organization.

## Chapter 1

### What Drives Cybercrime?



# Chapter 2

## How and Why Scams Survive, Thrive, and Succeed

**Fraud** is the criminal act of misleading and misdirecting a victim through trickery. Computer fraud, or **cyberscamming**, is a multi-billion-dollar industry that affects people and organizations around the world. Money is a powerful motivator, attracting greedy criminals and victims alike.

As technology changes, criminals adapt their strategies to reach new victims. In the past, criminals used manual processes to scam victims: mailing letters, sending faxes, and dialing calls. Today, modern technology simply puts a new twist on old fraud schemes. Now, the criminals use email, the internet, and messaging applications to reach their targets inexpensively and easily.

The global nature of the internet works well for cybercriminals. They tend to work from countries with loose or nonexistent laws against online crime or where violations are loosely enforced. A crook in Nigeria can target American victims via email; Romanian thieves can trap users through forged online bank sign-in pages; Mexican criminals can lure immigrants through text message spam. Most cybercriminals see online fraud as a nameless, faceless, fly-by-night crime that offers low risk and high reward.

In this chapter, you'll learn how and why scams thrive in the information age. Although victims of online fraud often lack security consciousness and online threat awareness, fraud isn't limited to the undereducated: smart, savvy people are also victims. Scammers succeed because they attack common human vulnerabilities: fear, greed, lack of skepticism, and too trusting.

### *The More You Try to Scam, the Better the Odds of Succeeding*

Every scam is a numbers game. A scam may fail because the target won't cooperate for numerous reasons, including distrust, caution, intuition, apathy, or suspicion. To succeed, a scammer must exploit human vulnerabilities, and to find ideal victims the scammer has to cycle through large numbers of people. For every thousand emails sent out, a criminal may get only a handful of replies—but only one or two replies could yield hundreds or thousands of dollars.

Like an aggressive car salesperson, a typical **con man** is pushy and persistent. Not every customer is ready to buy a car, and not every recipient is a willing victim of online fraud. Both the

## Chapter 2

### How and Why Scams Survive, Thrive, and Succeed

salesperson and the scammer understand this, and their persistence increases the odds of success. The more often a cyberthief attempts fraud, the greater his or her chances of success.

*The term con man is an abbreviation for “confidence man,” a swindler who gains a person’s trust or confidence for the purpose of fraud. Once trust is gained, a fraudster can more easily take the victim’s money.*

### **Persistence and Variety**

Scams are fragile things: just a little doubt, suspicion, or common sense can alert a potential victim and foil the fraud. However, because the odds of earning easy money from an online scam are fairly high and scammers only need one individual to fall for the scam, cyberthieves have motivation to persist.

Variety is also important to a successful criminal enterprise. A single scammer can run several scams and reap big money. In one scam, they may commit wire transfer fraud; in another, they might harvest sensitive information through targeted emails; in a third scam, they could prey on purchasing department personnel through a phony business-to-business (B2B) website.

Another scammer might commit identity theft to perpetuate other schemes such as healthcare fraud. Persistence and variety are successful attributes for any scammer. Online scammers, like fishermen, cast wide nets in several choice places to catch a lot of what they’re looking for.

## *A Successful Scam Spawns Countless Imitations*

Bernard Madoff didn’t invent the Ponzi scheme, but he is noteworthy because he mastered the method by defrauding supposedly sophisticated investors out of billions of dollars over decades using the same methods someone stealing a thousand dollars would use.

Scams survive throughout time (often through variations) not because they’re brilliant or clever feats, but because an endless supply of people act as victims. In his book [The Big Con](#), David W. Maurer writes of a saying among con artists: “There’s a mark born every minute, and one to trim ’em and one to knock ’em.” [6] In other words, there’s no shortage of victims (marks), crooks (those who scam others), and honest people (those who “knock,” or warn others, of a scam or try to stop it).

## ***Old Scams Finding New Victims***

A quote often attributed to P.T. Barnum states, “There’s a sucker born every minute.” Even though Barnum didn’t make up this idea, it’s as true now as when it was decades ago. We might even add to it: “. . . and that sucker makes a fine target for computer fraud.”

The following are just some examples of the variety of fraud currently in practice:

- ✓ Advance fee schemes
- ✓ Apartment deposit scams
- ✓ Bitcoin scams
- ✓ Bulk-mailing opportunities
- ✓ Business Email Compromise
- ✓ Business fraud
- ✓ CEO wire fraud
- ✓ Charity fraud
- ✓ Counterfeit money orders and cashier’s checks
- ✓ COVID-19 scams
- ✓ Craigslist scams
- ✓ Credit card fraud
- ✓ Email chain letters
- ✓ Facebook impersonation scam (hijacked profile scam)
- ✓ Fake antivirus software
- ✓ Fake ransomware traps
- ✓ Fake shopping websites
- ✓ Fictitious charities
- ✓ Fraud involving online auctions and classified ads
- ✓ Fraudulent cosmetics and “anti-aging” products
- ✓ Funeral and cemetery fraud
- ✓ GoFundMe scams
- ✓ Greeting card scams
- ✓ Health and life insurance fraud
- ✓ Hitman scam
- ✓ Identity theft
- ✓ Illegal sports betting
- ✓ Inheritance, laundering, and embezzlement scams
- ✓ internet auction fraud
- ✓ Investment schemes such as pump-and-dump and scalping
- ✓ IRS scams
- ✓ Job offer scams

## Chapter 2

### How and Why Scams Survive, Thrive, and Succeed

- ✓ Letter of credit fraud
- ✓ Loyalty points phishing scam
- ✓ Nigerian Letter or “419” Fraud
- ✓ Online automotive fraud
- ✓ Online dating scams
- ✓ Overpayment online scam
- ✓ PayPal and money transfer fraud
- ✓ Phishing and smishing (that is, texting through your phone)
- ✓ Ponzi schemes, pyramid schemes, and multilevel marketing
- ✓ Prime bank note fraud
- ✓ Reverse mortgage scams
- ✓ Romance scams
- ✓ Schemes that involve reducing credit card interest or debt
- ✓ Tech support online scams
- ✓ Telephone solicitation fraud
- ✓ Travel and vacation fraud
- ✓ Unexpected winnings scam
- ✓ Web service and credit card cramming (that is, billing for unauthorized services)
- ✓ Work-from-home schemes

The internet exposes new generations to modern twists on old scams. Before email was common, fraudsters abused mail and telephone services to defraud individuals and companies. Fraudsters sent get-rich-quick schemes as chain letters to mailboxes all over America. In its basic form, chain letter fraud uses a list of names and addresses with a request for the recipient to send money to those people. In return, the victim’s name and address is listed and circulated with the promise of exponential monetary gain. However, the financial benefit is actually earned by whoever orchestrates the scheme. Chain letter fraud persists in mail and email forms. Many victims are drawn to the prospect of a low-risk investment with high-yield potential.

*For the record, any chain letter is illegal if it requests money (or any item of value) and promises substantial return for all participants. See Title 18, United States Code, Section 1302, the Postal Lottery Statute. [7]*

As another example, despite being a well-known internet fraud, the **Nigerian scam** (also called the **419 scam** and officially known as an **Advanced-Fee Scam**) continues to operate decades after it first appeared, but it now has many modern twists. It still finds its way onto lists of top scams published by organizations like PCWorld, Symantec, Kaspersky, and PandaLabs.

*The Spanish Prisoner is a con game from the 1800s in which the victim is told of a wealthy but unnamed prisoner in Spain raising money to secure release. In return for investing, the victim is promised a generous financial reward upon release—a reward that doesn't exist. Sound familiar? It should. Modern variations include advance-fee fraud, the black money scam, the Russian/Ukrainian scam, and the Nigerian or 419 scam. The Nigerian scam employs the same trick by promising financial gain in return for funds advanced. Dozens of variations exist throughout different countries.*

Many modern scams are adapted from older schemes. Insurance scams are old, but criminals employ them in surprising new ways. Healthcare fraud costs an average of \$300 per year per U.S. taxpayer [8]. Medicare and Medicaid are defrauded in the millions; the single biggest Medicare theft exposed to date took nearly \$900 million [9]. On the heels of U.S. healthcare reform, senior citizens were being scammed by criminals preaching healthcare reform misinformation and peddling health insurance fraud.

## **Examples of Health Insurance Fraud**

Health insurance fraud is big business. In January 2020, 300 people including physicians, nurses, pharmacists, and physical therapists were charged with attempting to steal almost \$900 million. The Medicare Fraud Strike Force of 36 federal districts was involved and charges (civil and criminal) were filed against those accused [9]. Hundreds of fraud cases such as these are investigated and prosecuted each year by various federal law enforcement agencies.

Scammers are quick to capitalize on the irrationalities, fears, and knee-jerk reactions of desperate people, especially in uncertain times. State insurance regulators began to receive complaints about scammers selling “Obamacare” insurance policies in the wake of U.S. healthcare reform. It’s one of many tactics used to lure unsuspecting victims. Others include door-to-door sales of phony health insurance policies and useless medical discount cards. Obamacare insurance policies falsely claim that there’s a limited open enrollment period to purchase insurance as required by law, preying on ignorance and fear.

## **Simple Technology Tricks Reap Major Results**

Creating a web page is pretty simple. With some additional skill, many people can craft a convincing but bogus bank sign-in page or even a fake website that appears credible. A criminal with moderate coding skills can create, deploy, and remove a fraudulent site within minutes and vanish almost instantly. Sometimes they even copy the pages directly from a real website to make their fake site look even more authentic.

Simple scams are easy to execute and deploy. Sending fake emails to capture personal details is trivial. Some are so poorly constructed that they contain warning signs: bad grammar, poor

## Chapter 2

### How and Why Scams Survive, Thrive, and Succeed

spelling, and suspicious uniform resource locators (URLs). Other scam emails are very convincing. A complex scam may involve multiple criminals in numerous countries, layers of secrecy, and varying explanations and excuses.

*You'll see an example of an obvious email scam in Chapter 3, and another example that's highly believable in Chapter 4.*

Insa Nolte, an African studies lecturer in the United Kingdom, says that email transformed local fraud into the Nigerian scam. The scam began in the 1980s, at the decline of the once oil-based Nigerian economy. Unemployed university students created a convincing letter that drew the attention of greedy businesspeople wanting to make easy money. It spread to the West through letters and faxes, and then to entire companies. Copycat scams via email, Facebook, SMS text messages, and other social media eventually appeared throughout Africa, Asia, Europe, and the Americas.

### ***Trust Few, Share Little***

Fraud can very easily be perpetrated via email and text messaging. New users of technology tend to be trusting, so issuing fake emails is a simple, low-risk way to generate quick results. Customers often trust that only banks issue statements and that only banks know their clients. People often trust text messages they receive from sources claiming to be banks and financial institutions. Subscribers often trust fake services they receive by cellphone, believing that only the real company would issue such requests. These are easy assumptions to make, but they cost people millions in ruined finances and credit repair every year.

Many people are also too trusting in what they reveal and share online to a mostly anonymous audience. Well-crafted search terms can uncover a wealth of personal information to help cybercrooks target victims. This information is skimmed from blogs, social media such as Facebook and LinkedIn, and even government websites.

### ***How Technology Helps Fraud Schemes Evolve***

*Before email rose in popularity, most fraud was committed via mail and telephone. Charles Ponzi used the mail system in his famous scheme by taking advantage of foreign exchange rates. Nigerian scams were mostly local crimes until fax and telephone services spread them abroad. Email brings new life to old scams, as shown clearly with Ponzi schemes and Nigerian scams. Billions of nontechnical people use email, making them targets for fraudsters.*

## *A Little Knowledge Is Indeed Very Dangerous*

A little knowledge can be dangerous in the right circumstances. This statement cuts both ways: Knowing too little about online safety and security can be costly to victims in terms of damage to credit and credibility. On the other hand, a little insight into human nature often makes scammers successful.

For instance, humans are creatures of habit, and some are notoriously lazy. Many users choose passwords that favor convenience over security. For example, a typical user might use a weak password such as “password” or “123456” that is easy to remember and to type. Worse, some people compromise their own security by using the same password or similar passwords across multiple sites, including social networks, email accounts, and bank logins. Once a criminal obtains some credentials, he or she gains control over related assets. This can render significant damage and cause lifelong financial ruin to victims.

### **WARNING!**

*Efficiency helps accomplish a repetitive task with minimal effort, as when using weak passwords across sites. Weak passwords erode the strength of login security. If you reuse passwords, a criminal needs to uncover only one password to obtain all of your privileges. Even when a criminal does not target your accounts, he or she may guess your password while processing multiple accounts.*

## *Taking Advantage of Human Nature and Gullibility*

A swindler who commits fraud takes advantage of a victim through deceptive practices; the crook stands to gain personally or financially by stealing credit, identities, or finances. Fraud can affect just about anyone. Fraudsters are students of human nature. They understand common thought processes, habits, and behaviors. They know how to manipulate emotional vulnerabilities to pull off all types of scams. Success at one scam builds criminal experience that leads to other scams.

Many scams are successful because many people are overly trusting. Scams work because people can be successfully tricked into revealing personal information, transferring money, or relinquishing control. Some people remain gullible their entire lives; others eventually learn not

## Chapter 2

### How and Why Scams Survive, Thrive, and Succeed

to trust so freely. Finding a victim is simply a matter of cycling through groups of people to identify sufficiently vulnerable individuals to exploit.

*Online scammers target all the popular places: social networks, job boards, auction sites, online classifieds, dating sites, public forums, and everywhere else you go. Scammers know that such popular sites serve as major attractions that ensure a steady supply of potential victims.*

To depict all fraud victims as greedy, gullible, or stupid paints an inaccurate and incomplete picture. Even smart, well-balanced people are susceptible to fraud. Victims of Ponzi schemes are often honest, intelligent people made vulnerable through social and psychological factors. Social feedback—especially, word-of-mouth recommendations—plays an important role in the products and services people buy. When friends and coworkers share favorable or unfavorable experiences, their personal recommendations strongly influence the decisions of others around them.

Ponzi scheme victims are often bright people drawn to fraudulent investments by positive personal referrals from peers. And greed may not even be a factor. Friends of investors in Ponzi schemes are drawn to the sense of safety and excitement generated by strong social feedback. That's usually part of a scheme's design: Initial investors start small, get drawn further into the scheme, and unwittingly recruit other investors.

Anyone can be a victim of fraud, even an expert on gullibility or a well-informed investor. Sometimes scammers convince victims that they were specifically chosen for their honesty, integrity, or maturity. Because everyone is a potential target of fraud and because anyone can become a victim, there is no single personality profile that perfectly describes an ideal candidate for fraud.

### **Common Traits of Fraud Victims**

Dr. Stephen Greenspan, a retired professor of psychiatry, wrote a book titled [\*Annals of Gullibility: Why We Get Duped and How to Avoid It\*](#) [10], based on his 10 years of research into why people fall for schemes and hoaxes. Dr. Greenspan claims that everybody is vulnerable in certain situations. Even smart professionals and savvy investors can be fooled by complex math, exaggerated returns, and manipulative pitches. Even so, factors that increase a person's fraud risk include the following:

- **Extroversion:** An overinflated sense of confidence with a tendency to wander outside one's comfort zone. Extroverts are engaging and interactive, socially approachable, and willing to share personal information with others.



- **Gullibility:** A willingness to skip personal evaluations in favor of good social feedback. Gullible people refuse to acknowledge their poor judgment or mistakes and prefer that others take control.
- **Risk tolerance:** A personal comfort level with different kinds of risk. High risk tolerance gives people a “thrill of the unknown,” and all fraud schemes are high risk proposals that promise unlikely financial rewards.
- **Blind trust:** A habit of readily trusting the opinions of peers or strangers without proper evaluation. Transference of trust breeds false confidence, which can deter a person from being cautious.

### ***It Really Can Happen to Anyone***

*Days after publishing Annals of Gullibility, Greenspan found himself the victim of Bernard Madoff's massive investment scheme, which he attributes to social feedback. By targeting groups, Ponzi schemes seek to manipulate the transfer of confidence to lure other victims. Charles Ponzi, after which the scheme is named, was an Italian immigrant, like most of his victims. Promises of safe investments combined with false confidence fool investors into letting down their guard. It's easy to see how even bright, cautious people fall prey to fraud.*

\*\*\*

Fraud is one of many crimes that scammers commit online and offline. This book discusses many different types of internet-related crimes and how to protect yourself and your company from them. You'll learn how to recognize legitimate situations from bogus situations and get tips for avoiding problems.



# Chapter 3

## Types and Methods of Attacks

In this chapter, we will look more closely at the methods and mechanisms used to mount attacks for cyberheists. Along the way, we will also discuss how to avoid or deflect such attacks.

While reading this chapter, and when using the internet, keep the following in mind:

- Always be wary when dealing with unexpected email or when presented with links to web pages that you know nothing about. In far too many cases, such emails are trying to trick you into visiting a website and providing information that you should not divulge.
- Remember that simply visiting certain web pages opens the possibility of a so-called drive-by download that could install malware on your PC. This lets cyberthieves harvest information that you would otherwise not divulge.

### *The Social Side of Attacks*

A phishing email delivers a carefully crafted message designed to get its readers to download a file or click on a link that it carries. Some phishing messages rely on explicit threats to force action. These warn readers of account inactivation or cancellation or threaten financial losses, extra charges, and so forth. Other messages seek to cause alarm by reporting unauthorized account access, unusual withdrawals, or suspicious account activity. Still others inform readers about unclaimed funds, unexpected winnings, or prize awards.

In many cases of phishing emails, the message tries to get readers to click a link. Readers see further requests for information on the web page that appears after they click the link. Unfortunately, it may already be too late to avoid trouble, even if the user immediately closes the page. What makes such access dangerous is that simply visiting the page can trigger a drive-by download (a malicious software download) to the user's PC, after which the software installs a Trojan. Trojans can collect all user keyboard activity and send it elsewhere across the internet to a cyberthief, encrypt the data on the hard drive, and hold it for ransom, or perform any number of malicious actions.

## *You've Been Engineered ... Socially, That Is!*

Social engineering is the term information security experts use for the act of talking somebody into divulging information that they shouldn't share with an unauthorized third party or performing some other action. Clever scammers rely on human impulses to be helpful, to avoid trouble or conflict, and to try to fix things when they break to extract information from unwitting and unwary users.



### **Social Engineering**

Techopedia.com defines social engineering as “deception for the sole purpose of gathering information, fraud or system access” [12] and Webopedia.com adds, “the act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information.” [13] Wikipedia, on the other hand, defines social engineering as the “psychological manipulation of people into performing actions or divulging confidential information.” [14]

The key elements of social engineering reveal themselves in some of the words from those definitions: deception, fraud, and manipulation. Cyberthieves try to set up and define a situation where it will seem natural, normal, or helpful to provide the requested information or to click the link that's displayed. For non-email attacks, especially on social media such as Twitter or Facebook, all that's necessary is to present an attractive reason to get people to click a link. This, too, is social engineering.

The sections that follow take a closer look at some phishing attacks to show where the social engineering comes in. You'll get a chance to see how social engineering is designed to get a response from readers. Even if readers don't provide the requested information, clicking the link is good enough to give cyberthieves a “foot in the door.”

### ***Social Engineering Tools and Tricks***

Cyberthieves rely on creating a sense of urgency in their victims. Phishing messages are designed to get victims upset, edgy, or anxious, so that they will respond immediately. Cool deliberation is nowhere in this picture—by design.

Many phishing messages start by presenting a situation and then explain the consequences of delay or inaction. Next, they present a link or propose a much-needed action to fix that situation, and they often close by promising dire outcomes if the reader does not take immediate action.

For example, consider this message purportedly from Google Gmail regarding unused accounts:

Due to the congestion in the Gmail system, Gmail will shut down all unused accounts. You must confirm your email by filling out your login information below and then clicking the Reply button. Failure to do so within 24 hours will result in account suspension.

This message contains all the social engineering elements of a typical phishing attack:

- Account congestion and removal of unused accounts are cited as reasons for sending the email.
- Readers are instructed to confirm their email by filling out their login information.
- Readers are asked to click a Reply button (a hypertext link to the phishing site).
- Readers are informed that failure to comply with the request will result in account suspension and loss of access to their email.

It's easy to see that the cyberthieves are looking for account and login details. They play on the human tendency to be helpful and to help create order (for example, by reducing account congestion and getting rid of unused accounts). They give the reader little choice but to click the Reply button, threatening account suspension for a failure to comply. All this adds up to a calculated appeal to get readers to provide the information or perform the actions the cyberthieves want and to click the link.

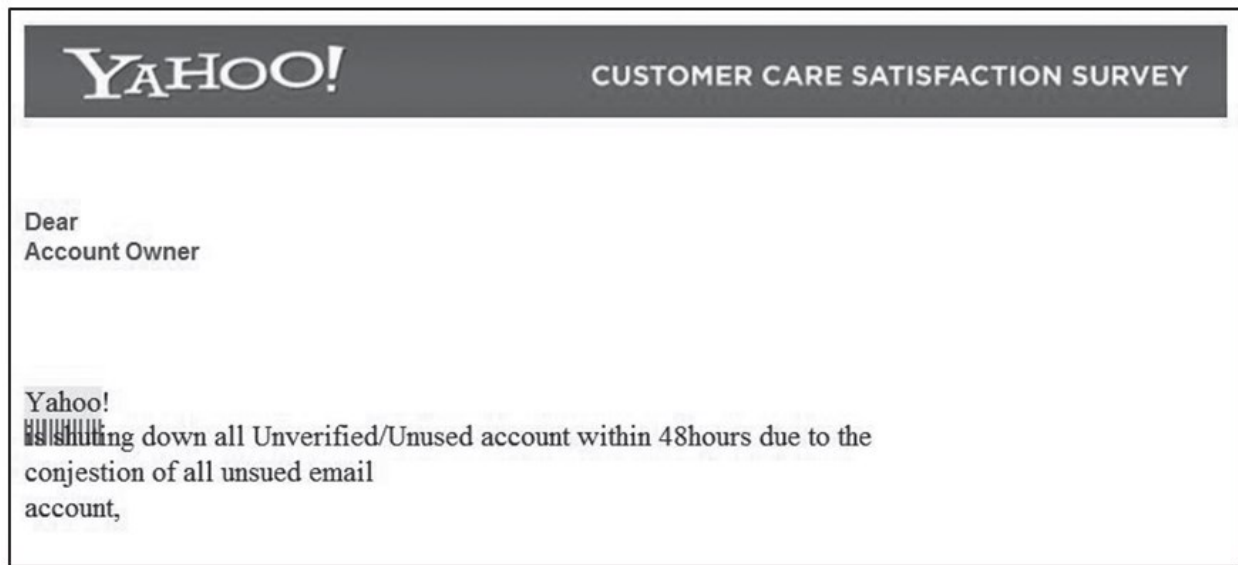
### ***Stressor Event***

*According to Wikipedia, a stressor is a chemical or biological agent, environmental condition, external stimulus, or an event seen as causing stress to an organism.*

*Psychologically speaking, a stressor can be events or environments that individuals might consider demanding, challenging, and/or threatening individual safety. [11]*

## *Anatomy of a Blatant Phishing Attack*

Email is the favored medium for phishing because it lets users click embedded links. Figure 2 shows a blatant and low-grade phishing attack. It further illustrates social engineering techniques used in related emails.



***Figure 2 Snippet from a Hypertext Markup Language (HTML) phishing message***

The remainder of the email message asks for personal information, such as username, password, date of birth, occupation, and country of residence. The message sets up the urgency to provide the information by stating “Failure to comply means your Yahoo! email account will be deactivated without further notice.”

Just the small snippet shown in Figure 2 contains several telltale signs of a phishing attempt:

- It’s addressed to “Account Owner” rather than to an individual. Yahoo has enough information to address each recipient by name, and it would do so if it were the actual sender of such a message.
- There’s a strange formatting error in the first paragraph of the message. The Yahoo! text graphic includes a shaded background with vertical strokes beneath that intrude on the text in that line. Likewise, odd line breaks follow after “Dear” and throughout the message body.
- The font used for the message salutation is very different from the font used for the message body (sans serif versus serif); Yahoo’s own email messages use consistent fonts throughout.

- The message body text omits a space between “48” and “hours,” and it misspells “shuting” (shutting), “conjestion” (congestion), and “unsued” (unused).
- The Yahoo! graphical header at the start of the snippet references a customer care satisfaction survey, but the message body isn’t associated with a survey or attributed to customer care. Yahoo would not do any of this.

In this message, the outright errors, formatting glitches, and strange mix of graphical and badly written textual elements point toward a phishing attempt.

## Examining the Source Code

Now, let’s take a quick look at the source code for the incoming HTML-formatted message. (To see it, you just click something like **View > Page Source** if reading email in a web browser.) Figure 3 shows a part of the message header from the phishing message shown in Figure 2.

```
X-YahooFilteredBulk: 82.132.130.169
Received-SPF: none (mta161.mail.sp2.yahoo.com: domain of
mailservice@yahoo.com does not designate permitted sender hosts)
Received-SPF: none(yahoo.com: yahoo.com does not designate permitted sender
hosts)
Received-SPF: DomainKey Not Present
```

*Figure 3 A snippet from the message header shows that something is up!*

Notice that the originating IP address for this message is 82.132.130.169. A quick trip to the [IP2Location.com](http://www.ip2location.com) website reveals that this address is in the United Kingdom and comes from an internet service provider (ISP) named O2 Online. If the message were legitimate, Yahoo would contact readers from the United States, and it would not originate its messages at a service provider that specializes in broadband and mobile phone accounts for consumers. (Yahoo uses Inktomi, as you’ll see later in this section.)

*The IP2Location.com website lets you know the physical location of the ISP associated with any URL through its IP address. You simply PING the domain name to get its address.*

*See <http://www.mediacollege.com/internet/troubleshooter/ping.html> for a quick tutorial on the PING command.*

Furthermore, the claimed Sender Policy Framework (SPF) identification is attributed to mailservice@yahoo.com, but Yahoo reports that it “does not designate permitted sender hosts.”

## Chapter 3

### Types and Methods of Attacks

This means the claimed originator does not match the actual originator, and that the email address has been **spoofed**.

Further down in the message header, the text shown in Figure 4 appears. This text shows that the purported Message-ID, Reply-To, and From fields in the message as it displays in a web browser have all been faked. The less-than and greater-than symbols (< and >, respectively) make the enclosed text look as if the message originates from Yahoo, includes a Yahoo reply-to address, and comes from mailservice@yahoo.com, but all these entries are bogus.

```
Message-ID: <4C63A9A32EA52BFA@> (added by '')  
Reply-To: <alertsevice25@yahoo.com.cn>  
From: "Yahoo Service"<mailservice@yahoo.com>
```

**Figure 4** *These Message-ID, Reply-To, and From addresses are carefully faked*

Finally, there's a dead giveaway at the end of the message header (see Figure 5), where fields that begin with "X-SA" appear to indicate why this message has been flagged as spam. Spam Arrest, the spam-filtering service where we pick up some of our incoming email, labels the message a forgery.

```
X-SA-MPREASON: Forgery
```

**Figure 5** *The spam-filtering service detects that this message is a forgery*

Spam Arrest deduced the forgery from the mismatch between the actual point of origination (82.132.130.169) and the claimed point of origination (mailservice@yahoo.com). Yahoo's actual mail server address is 68.142.198.147; this real address appears in the email header for the Yahoo mail server that processed this message. IP2Location reports that 68.142.198.147 is in Sunnyvale, California, and operated by Inktomi Corporation for the domain name yahoo-inc.com, which is entirely legitimate—and different from the actual point of origination.



### Spam

**Spam** is unsolicited and unwanted email, usually sent in bulk to thousands of email addresses. Spam emails generally try to perpetrate some type of scam, such as selling fake medicine, or seek to verify live email addresses to which other spam may later be sent.



## *The Technical Side of Attacks*

What happens when someone reading a phishing message clicks a link it contains? It doesn't matter if that link is in an email, in a Tweet, or on a Facebook or other web page. What matters is what happens when the user's web browser follows that link and opens the page on the user's desktop or other device window.

### ***Disguise and Conquer***

Chances are very good that when a phishing page opens in somebody's browser, it will be a convincing imitation of the website it claims to be. After all, anyone can grab the source code for any web page online, as well as the graphics that go with it, so it's trivial to create a web page that looks and feels much like the original.

Nevertheless, phishing sites often differ from the originals they imitate. As we saw for phishing emails, you'll notice occasional formatting glitches. Likewise, you'll often see font or typeface mismatches. Sometimes odd combinations of headers and graphics will occur, as with the "Customer Care Satisfaction Survey" in the example shown in Figure 2. Noticing any of this requires a keen eye and a willingness to scrutinize small details. Many ordinary web users are oblivious to such details.

### ***Hidden and Malicious Payloads***

By the time a user gets to a phishing page, he or she may already be in trouble. That's because many such pages try to automatically install malware on any unpatched PCs that come to visit. On unpatched computers, these downloads occur without requesting user permission to proceed; in fact, they don't even inform users that they're occurring.

*These downloads are called drive-by downloads because simply loading a web page causes them to occur. See Chapter 1 for a complete definition of this term.*

In most cases, drive-by downloads rely on active content to work inside a web browser. **Active content** means that there's code inside one or more objects on a web page so that downloading the page can cause the code associated with such objects to be downloaded as well. Active content comes in many forms. Modern browsers use HTML5 and JavaScript, which are built into the browser itself. Older obsolete technologies include:

- ✓ ActiveX controls or applications, a Microsoft technology that's mostly associated with Internet Explorer (an obsolete browser that should not be used).
- ✓ Java applets, which requires a special browser add-in to work but is widely available for most web browsers.

## Chapter 3

### Types and Methods of Attacks

- ✓ Adobe Flash is often used by older websites for active content but is rapidly being replaced by HTML5.

All these forms of active content—and more—can be used for both legitimate and safe applications and illegitimate and unsafe uses. Unfortunately, the shady variety is what usually infects devices such as PCs, smartphones, and tablets that visit phishing sites.

### ***The Mechanics of Drive-By Downloads***

When a browser downloads a page to a computer, it interprets the hidden instructions that govern how the web page is to be displayed. It also interprets and executes objects it finds referenced in those instructions. In general, this is how web pages handle active content. In particular, this is how the hidden instructions to download malicious active content can sometimes move onto an unpatched PC. Even when anti-malware software is present, some malware is not readily identified and can still get around a PC's defenses. When that happens, the malware installs itself on the visiting, unpatched, PC.

Normally, drive-by downloads are made possible because of unpatched browser addons such as Java and Adobe Flash, as well as malicious browser extensions. Every extension should be considered an additional attack vector. Review them to determine if they are needed, up to date, and come from a reliable source.

Trojans are malware programs designed to perform unauthorized actions. They can use the internet to establish backdoor connections to other machines and send them files and information. When cyberthieves gain access to the data on computers or smartphones, they use it to make fraudulent bank transfers, misappropriate credit card funds, and do anything else programmatically possible to steal their victims' assets.

### ***Information Harvesting***

Phishing attacks often include an outright appeal for information from victims. Think of the items requested in the Yahoo phishing attack cited earlier in this chapter: name, password, date of birth, occupation, and country of residence. Someone who provides that information is inviting identity theft as well as providing data about a specific email account.

Phishing has become more sophisticated over the years. The threats were initially quite simple: entice a user to click a link in an email or other document. This would go directly to a web page that attempted to get the user to enter their credentials. It was relatively easy for security tools to block these attempts because the links were very recognizable.

The bad guys didn't sit on their laurels and began using redirectors to obfuscate web page URLs. When a user clicked on one of these URLs, it was translated to the URL of the phishing webpage.

As security software caught onto this trick, multi-stage attacks appeared. The user is enticed to click on a link and is directed to a normal looking, non-intrusive web page. From here, the user performs something, which results in the download of an HTML file onto their system or device. The user is encouraged to click on a file (which may have been placed on their desktop), which launches yet another HTML page with a link to finally send them to the phishing web page. That page could do anything from downloading a trojan, including installing a keylogger, to infecting the system with ransomware. Security software has a more difficult time detecting these types of multi-staged attacks. [15]

## **Malvertising**

Online banner advertisements have come a long way since the days of simple text or, at most, a brightly colored image. Today's online ads are rich with Flash, JavaScript and other application code to dazzle viewers and engage shoppers. Unfortunately, this has introduced the ability of cybercriminals to inject malicious code into the advertisements. Thus, the simple fact of viewing a banner ad can lead to an exploitation by malware, using techniques like the drive-by download discussed earlier. These method of infecting systems with malware is known as **malvertising**.

## **CEO Fraud**

In a form of phishing known as **CEO Fraud**, criminals target specific organizations and seek to directly exploit the computer of the CEO (or other high-level manager). Once malware has been slipped onto their victim's computer, the criminals observe the habits and styles of that CEO, building up a profile of how he or she operates, writes, sounds, and acts. After weeks or even months, often when the manager has gone on vacation or a business trip, they send out malicious emails and letters to other employees or customers written exactly in the style of the CEO. For example, the CFO might receive an email, seemingly from the CEO, ordering a million dollars to be transferred or paid. Since the order appears to be valid, the CFO probably will perform the fraudulent transfer, and no one will be the wiser until a much later date. Often, the returning CEO has no idea what happened, and no one goes out of their way to mention it since they thought it was all normal business. The fraud can be discovered because of a hundred different reasons, only one of which is by the CEO themselves.

## **Webcam Hijacking**

Most laptops and tablets include built-in webcams, which is very convenient for teleconferences and so forth. However, once cybercriminals take over a machine, they control these cameras and can use them to view and record anything going on near the computer. This opens up the possibility of blackmail and espionage by surreptitiously recording the activities of whoever is in the room.

## ***Other Attack Vectors***

BYOD, or **Bring Your Own Device**, is the concept that employees use their own smart phones, tablets and laptops for their work instead of being provided that equipment by the company. This introduces new concerns and that those devices are not under the control of the company and may have inadequate security. For example, a user could plug their smart phone into their work computer and infect it with a virus, or they may join the wireless network in their company and introduce malicious software to the network.

You've probably seen new devices referred to as smart light bulbs, smart sockets, and smart home alarm systems. These devices, known as the **Internet of Things (IoT)**, can be programmed to do a variety of things which are very convenient. For example, a smart lightbulb could be programmed to automatically turn on and off at certain times of the day. Each of these devices contains a computer component which often can be programmed via the internet. It's possible for hackers to break into these devices and reprogram them for their own purposes. An internet ready smart video camera could be used by a hacker for surveillance or blackmail purposes, or an intelligent alarm system could be remotely turned off by criminals. The security defined for these devices is not yet mature and they should be used with caution in the workplace and at home.

## ***Cryptocurrencies***

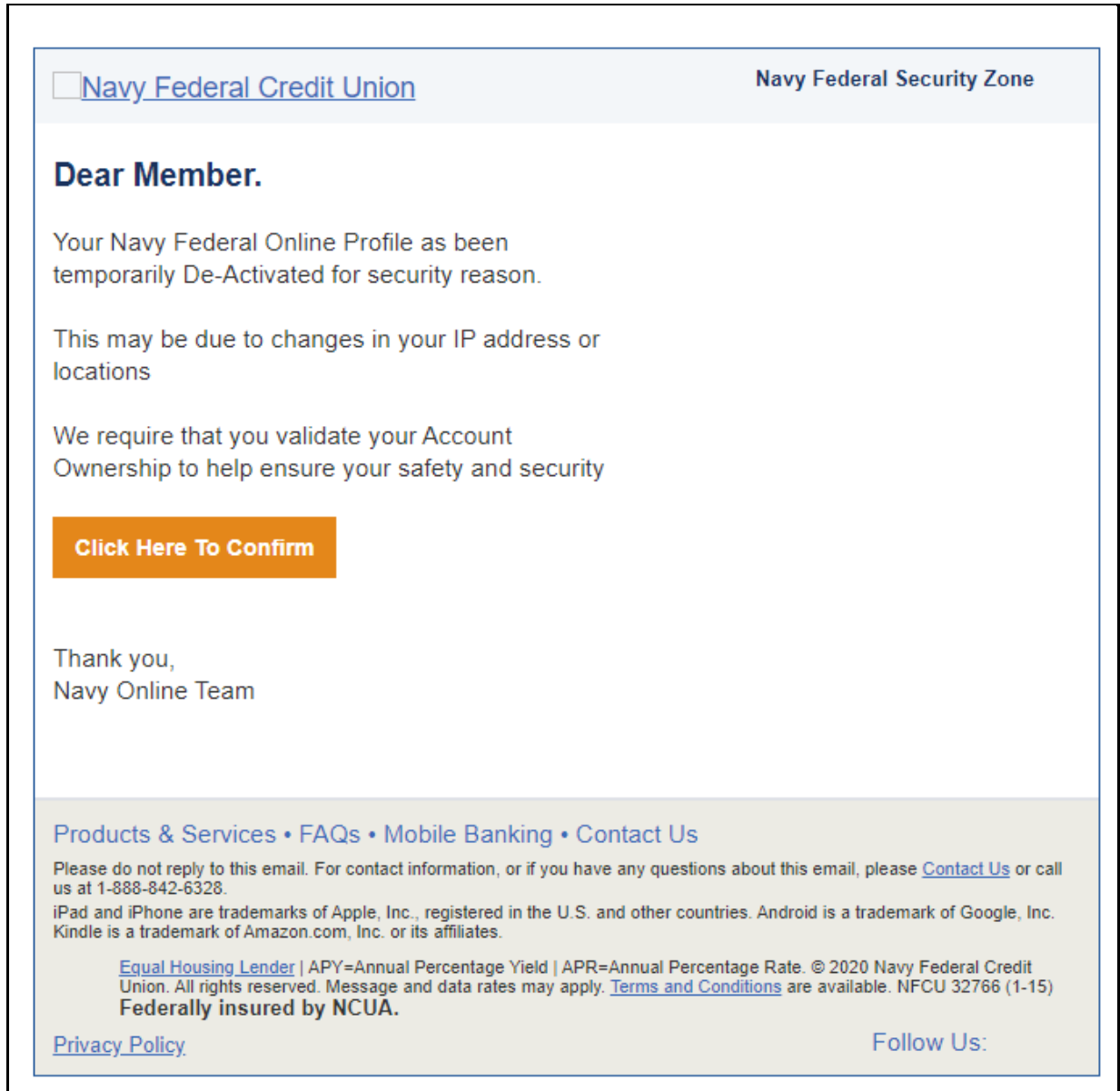
Bitcoin and other **cryptocurrencies** are growing in popularity. They are created and held electronically, no one controls it, and there is nothing to print. They are produced by people and businesses on computers throughout the world.

Several million people are now using cryptocurrencies of all types, with over 400,000 transactions per day. [16] These currencies are often unregulated and have often been designed to be used anonymously. The value of all bitcoins in circulation as of November 201 was \$146 billion. [17]

The bad guys go where the money is, so with numbers like this, phishing attacks targeting Bitcoin users are literally "phishing expeditions." Attackers have used lists of known/active Bitcoin users and used widespread misperceptions about Bitcoin to try and improve their odds of success. Also, because of its anonymity, ransomware often demands payment be made in bitcoins or other cryptocurrencies. Once payment has been made, the bitcoins are extracted or laundered using various techniques, so it is virtually impossible to track. The availability and default anonymity of cryptocurrencies caused an explosion in ransomware.

## Example Scamming and Phishing Emails

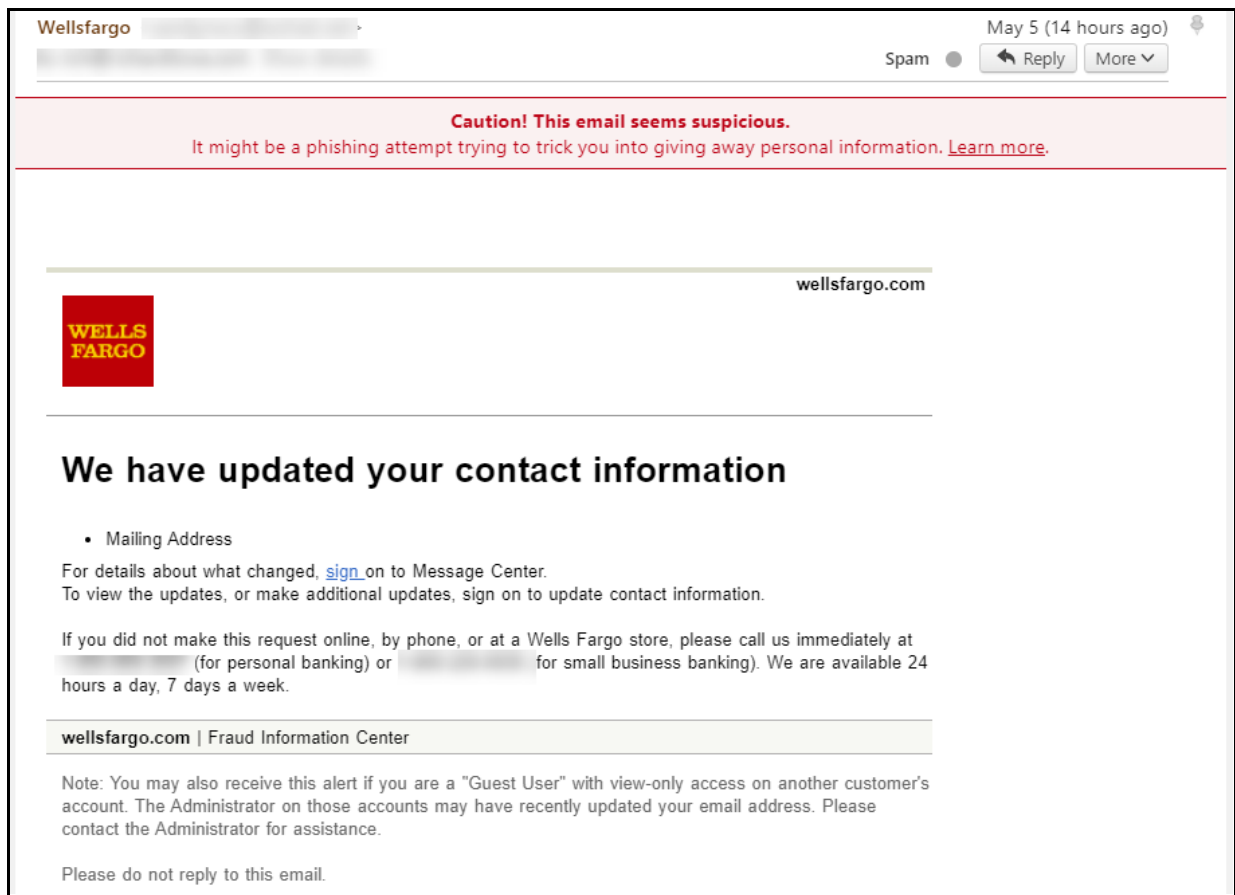
Some samples of scamming and phishing emails are shown below. We'll discuss these techniques later in this book.



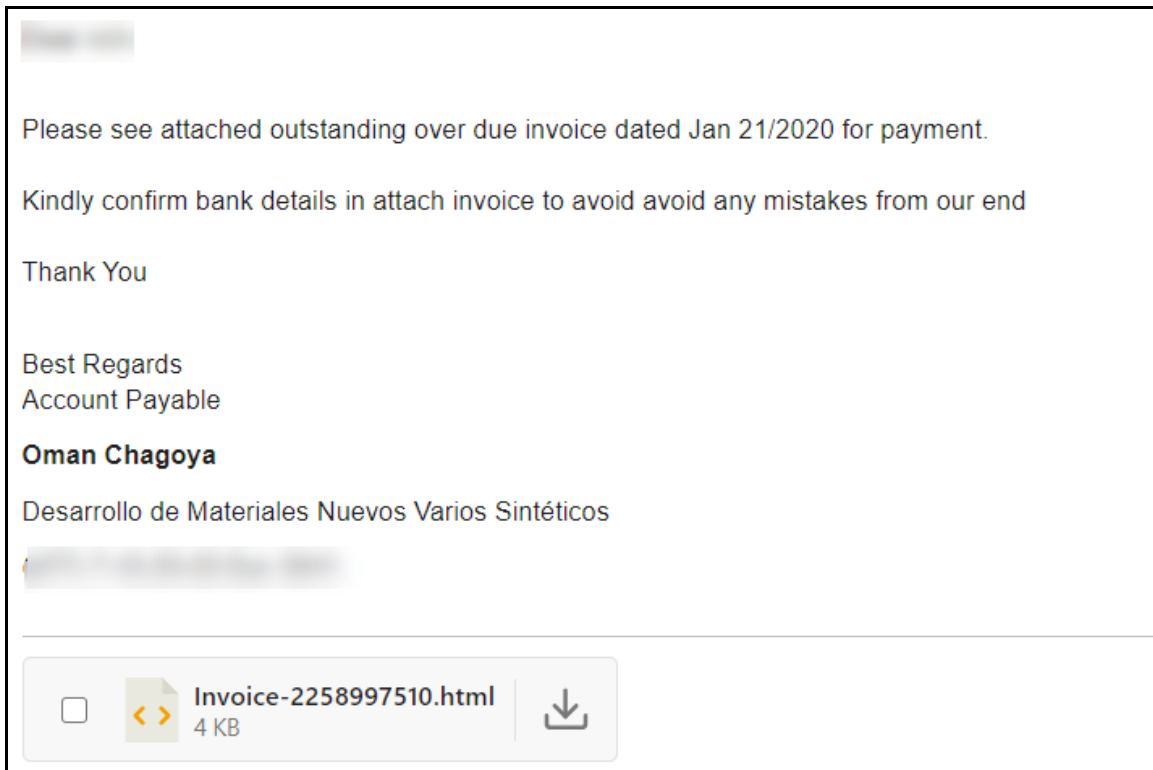
**Figure 6 Sample Phishing Email**

## Chapter 3

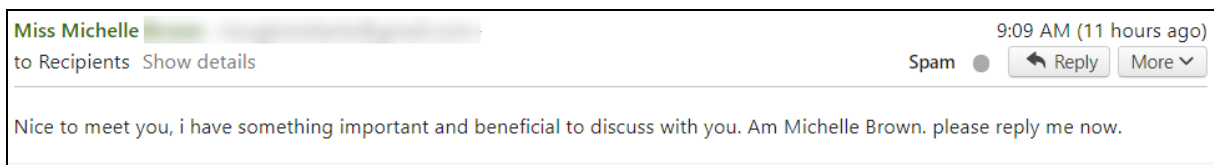
### Types and Methods of Attacks



**Figure 7 Phishing Email**



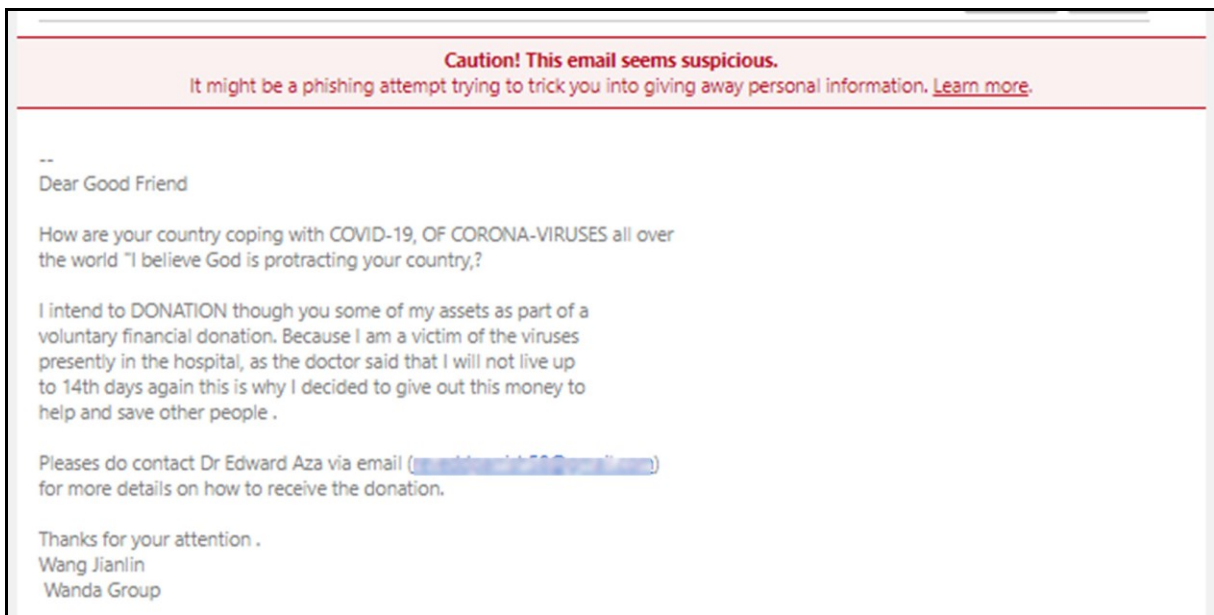
*Figure 8 Phishing Email*



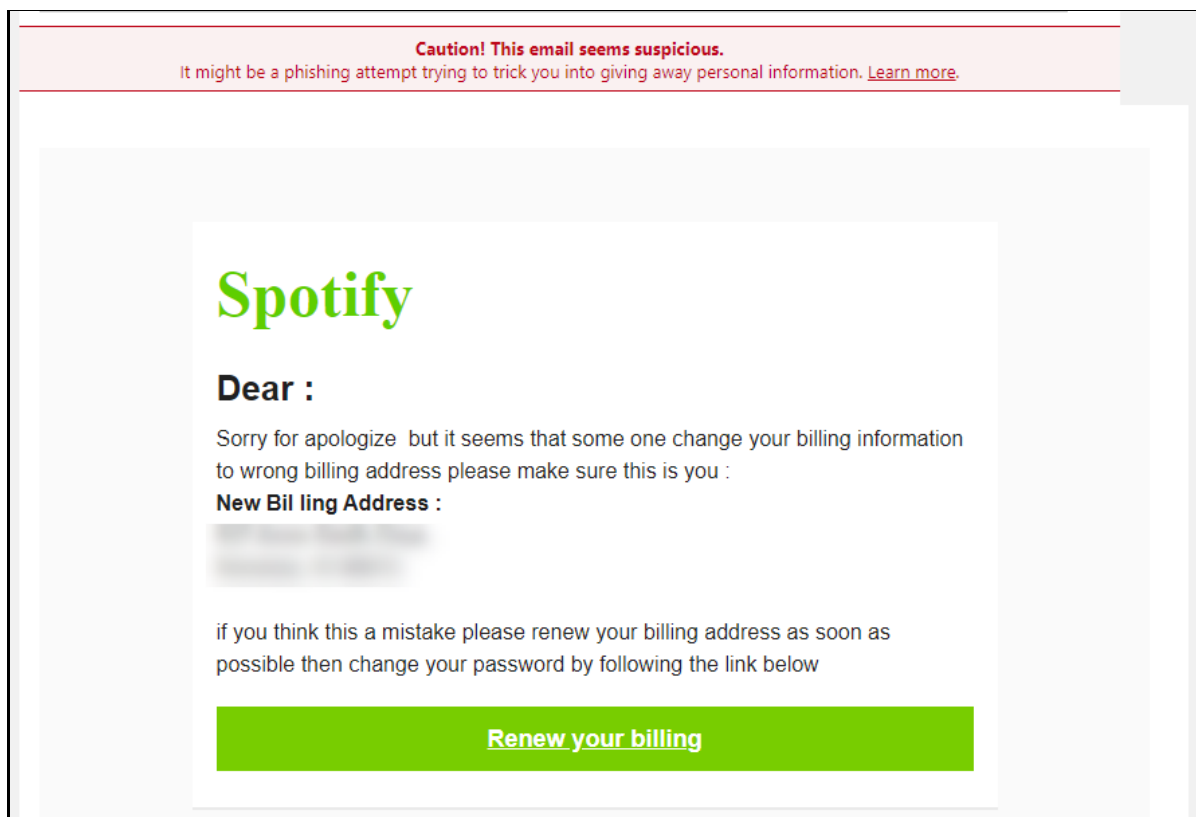
*Figure 9 Advanced-Fee Scam*

## Chapter 3

### Types and Methods of Attacks

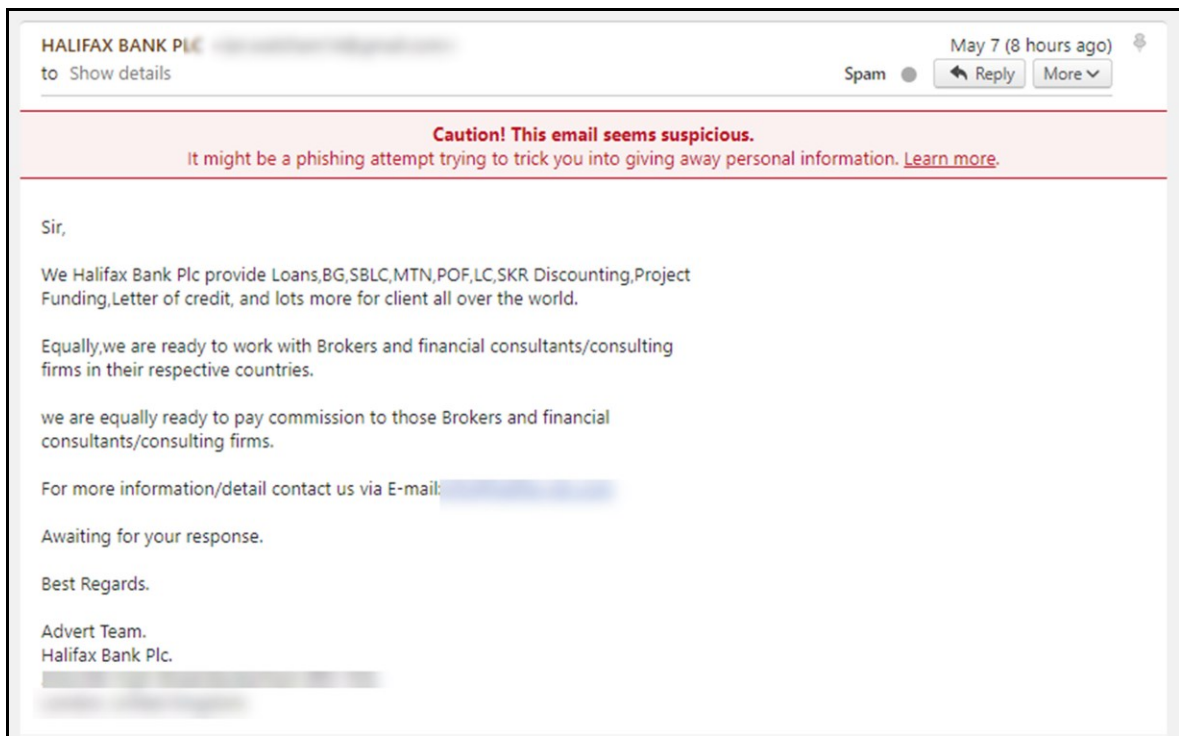


**Figure 10 COVID-19 Scam**



**Figure 11 Phishing Scam**

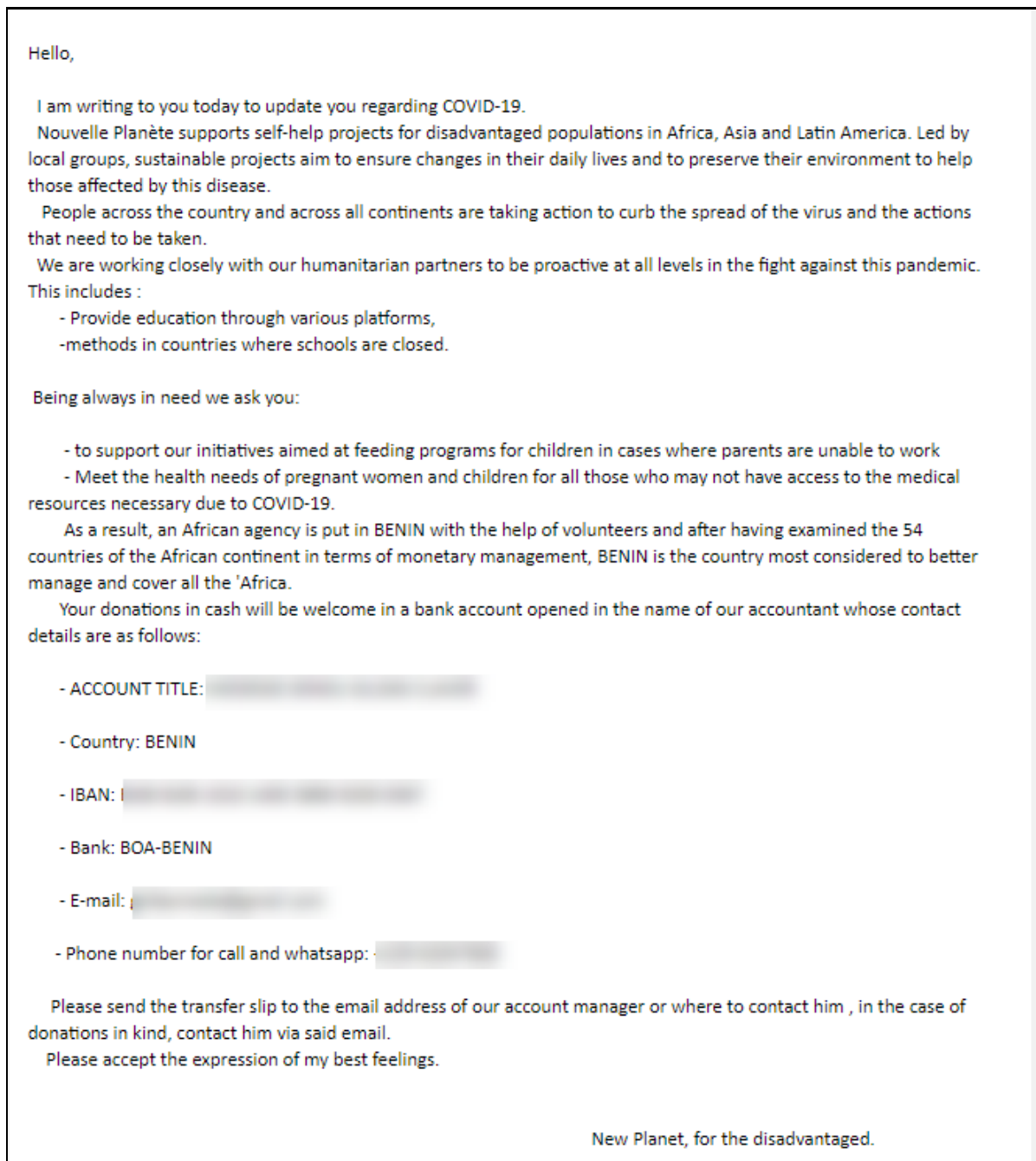




*Figure 12 Typical Advanced-Fee Scam*

## Chapter 3

### Types and Methods of Attacks



**Figure 13 Charity Scam**

\*\*\*

Attacks attempt to penetrate your business and defenses using a wide variety of tactics. Assume people can be manipulated via social engineering, your webcam or audio can be hijacked, and

online advertisements can contain malicious code. These and other attack vectors must be understood before you can begin to build the appropriate defenses.



# Chapter 4

## Phishing Explored and Explained

Phishing is a play on its sound-alike source word, fishing. The first recorded use of the term phishing appeared in 1996, when a team of hackers scammed AOL usernames and passwords from unsuspecting users. These unwilling and unwitting pioneers received official-looking email messages that requested account information and gave a reasonable (but bogus) explanation for the request.

A surprising number of AOL users “bit” and provided their account information to the hackers. Various reports from that period say enough accounts were harvested to turn these “phish” into an unofficial currency among hackers. They would trade some number of phish for a piece of software or trade one group of phish for another, as they saw fit.

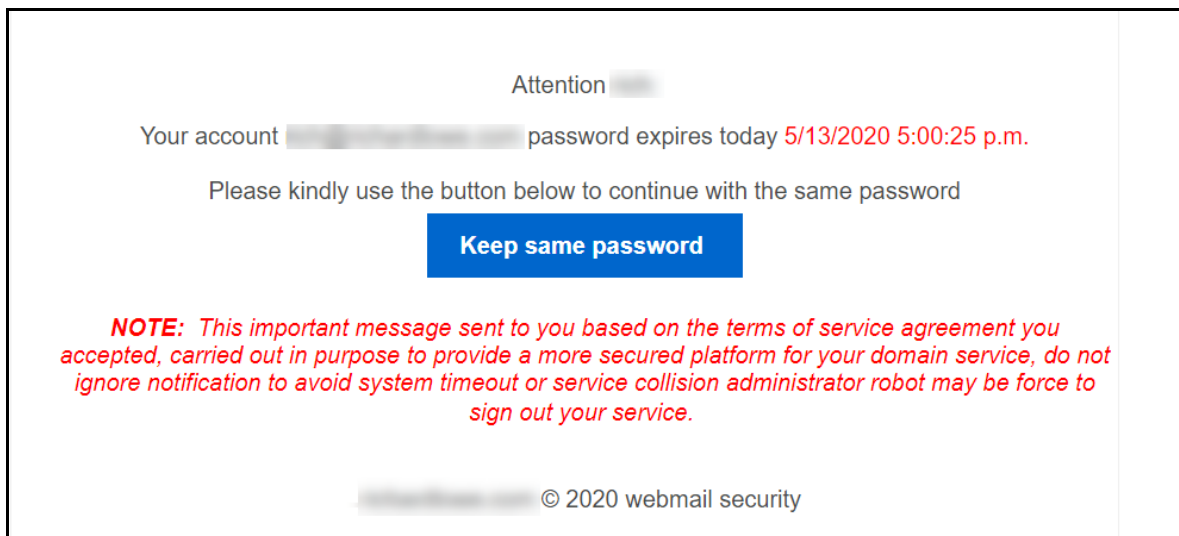
One of the earliest reports of phishing showed up in the media on March 16, 1997, in a story printed in the Florida Times-Union newspaper. It contained the line “The scam is called Phishing, as in fishing for your password, but spelled differently.” Since then, internet users have endured almost two decades of phishing attacks, mostly via email. In the past few years, however, the growth of social media such as Facebook and Twitter have prompted proliferation of phishing attacks via posting or Tweeting.

### *The Basic Laws of Phishing*

When it comes to creating and maintaining user awareness of phishing, it’s often helpful to break this form of criminal activity into its most basic components. A trio of terms captures just about every phishing attack we’ve ever encountered: imitate, motivate, and act (click a link, reply to an email, or whatever). We therefore refer to these three actions as “the basic laws of phishing.” The following sections spell out these laws in some detail. Figure 14 shows an example phishing email.

## Chapter 4

### Phishing Explored and Explained



**Figure 14 Typical phishing email**

### **Imitate**

Imitation is the impersonation part of the phishing attack. An email phishing message strives to look like it comes from some particular organization or individual. It may use the same fonts and the same logos to make itself appear legitimate. In short, many attackers try hard to make their messages look real and convincing. Sometimes the results are laughable, but other times they're very believable. However, even superficial examination of the header for such a message will show that the Sender (or From), Reply-To, and other standard email fields all point to impersonation.

### **Motivate**

Motivation is the social engineering part of a phishing attack.

- ✓ A message may report that information has been lost or is missing; this type of message plays on a victim's desire to be helpful and solve problems.
- ✓ A message might inform its readers that an account will be canceled or suspended if they don't cough up the requested information; this type of message plays on recipients' natural desires to protect their accounts or assets or to keep enjoying accounts and services that they like or want.
- ✓ A message might also indicate that until problems are addressed, and information is provided, the victim can't use payment services or pay pending outstanding balances. Such instructions play on a reader's emotions, and seek to exploit human instincts to help others, avoid trouble, or fix things when they break.

All these messages are sent for one purpose: to get readers to take action as requested in the message, Tweet, or Facebook post. All these threats, promises, and consequences are designed to provoke action from their readers so that attackers can obtain their confidential data.

## **Warning!**

*Most email applications don't show images by default unless you enable it in the settings. This means images show as placeholders in the email message. Don't show or load images by default because by doing so, the scammer learns that you at least looked at their email message and confirms your email address as valid and active. They then know they can keep sending you messages and sell your email address to other scammers and phishers because you've proven there is a human being reading their message.*

## **Take Action Now!**

The visible hook in a phishing attack is the form that users are requested to fill out. This is where they provide the details that cyberthieves are after to access their accounts and to steal or spend their money. To access this form, users must act (click a link, send a reply, or whatever) in response to a phishing message, Facebook page, Tweet, or post from other social media.

An invisible hook may also lurk in a phishing attack. That is, the phishing page that a victim visits may cause a drive-by download of malware if the user is using an unpatched application. If that happens, even users who don't bite the visible hook and fill out the form may still fall prey to the invisible hook if the malware download succeeds. The victim is then stuck with some kind of malware, like a keylogger and a backdoor Trojan, that he or she may not know about for some time.

*Oracle Java, Adobe Flash, malicious extensions, unpatched browsers, and obsolete browsers are the primary reasons for the success of drive-by downloads. Fully patched, modern browsers without these applications and problems provide good protection from drive-by downloads. The lesson? Don't use older browsers, always keep up to date on patching, verify extensions, and don't use Oracle Java and Adobe Flash, if possible.*

Most users run some form of antivirus and antispyware software on their PCs nowadays. This should protect them from known, previously identified, forms of malware, but it may or may not protect them from new or unknown forms. Although antivirus programs are a needed tool in any defense-in-depth computer defense program, no antivirus program is a hundred percent reliable.

*No device (PC, smartphone, or tablet) is entirely safe from malware, so avoidance (don't reply to the email or click the link!) and being fully patched remains the best practice.*

## *Attack Anatomy 2: A Well-Done Phish*

In Chapter 3, we analyzed a rude and crude phishing attack on one of our Yahoo email accounts in a section titled “Anatomy of a Blatant Phishing Attack.” We deliberately showed a poorly done attack, to show that it’s a wonder that some phishing attacks can succeed at all. Indeed, that particular example was rife with formatting errors and misspellings—obvious signs that the message couldn’t possibly be legitimate.

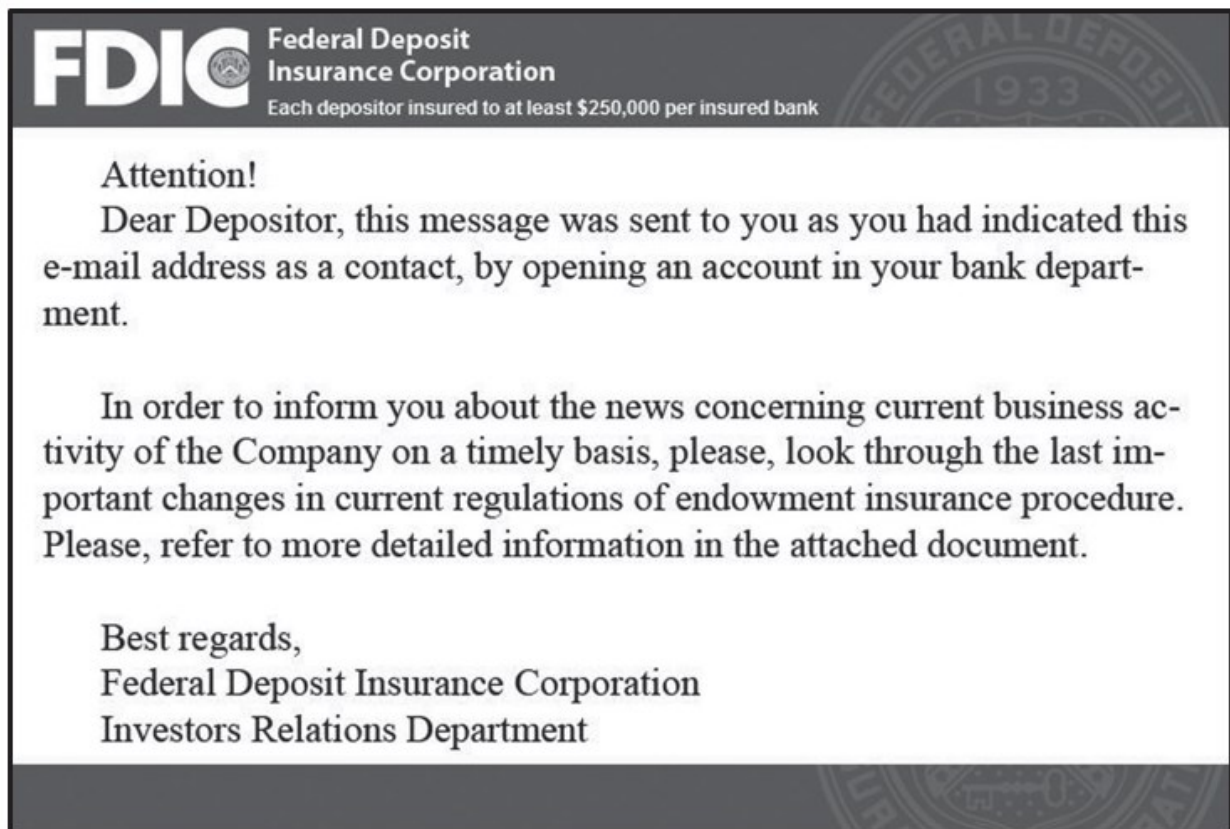
In this section, we examine a more polished phishing attack message below that uses the Federal Deposit Insurance Corporation’s own logo and banner artwork (see Figure 15). It’s nicely laid out and formatted, and it contains no misspellings—but it does contain two surprises. Only a few subtle grammatical errors provide telltale clues that all is not as it seems here. In the next sections, we inspect this ticking time bomb closely to explain its dangers.

### ***The First Surprise: Steganography***

The entire body of the message shown in Figure 15 is a single graphic. It is located on the blog page for a hosting provider’s server based in Ireland (webcore.ie). Interestingly, this graphic appears nowhere in a blog on that server, and an internet search on the graphics file name (fdic\_finish1.gif) turns up nothing useful. With no obvious connection to the message, something mysterious and probably illegitimate is going on here.

Further searching online turns up two examples of this message at the spam reporting site spamigot.com. We used the jsunpack JavaScript Unpacker utility to analyze the image and found that the original image, disturbingly, contains 22,349 hidden bytes of data out of a total of 36,981 bytes of content. In other words, only about one-third of the bits in this image are needed to paint the image on the screen, and the other two-thirds are unrelated and might possibly have sinister intent.





*Figure 15 The message itself is only an image, but it contains two surprises.*

There's a word to describe what could be at work here: steganography. Jsunpack reports that there are no "malicious or suspicious elements" in this particular image file, but there very well could be! My guess is that a less-than-expert cybercrook tried to craft a malicious payload inside the image but failed to create a working implementation. Nevertheless, the image certainly looks good, even if it doesn't work the way its creator may have wanted it to. So, the first surprise in this phishing message is that the nicely crafted image that makes up the body of the message is carrying hidden freight. Fortunately, technical analysis of that freight shows that it contains nothing of a suspicious or malicious nature.



### **Steganography**

**Steganography** has Greek roots that mean "covered writing." The Greeks sent secret messages between parties by covering up those messages so they couldn't be seen without removing an obscuring layer from the message. Today, steganography refers to the deliberate concealment of digital information within other seemingly harmless messages or digital objects, such as graphical images.

Steganography replaces useless or unused bits inside ordinary computer files with bits that make up some kind of message, information, or even executable code. The files in

## Chapter 4

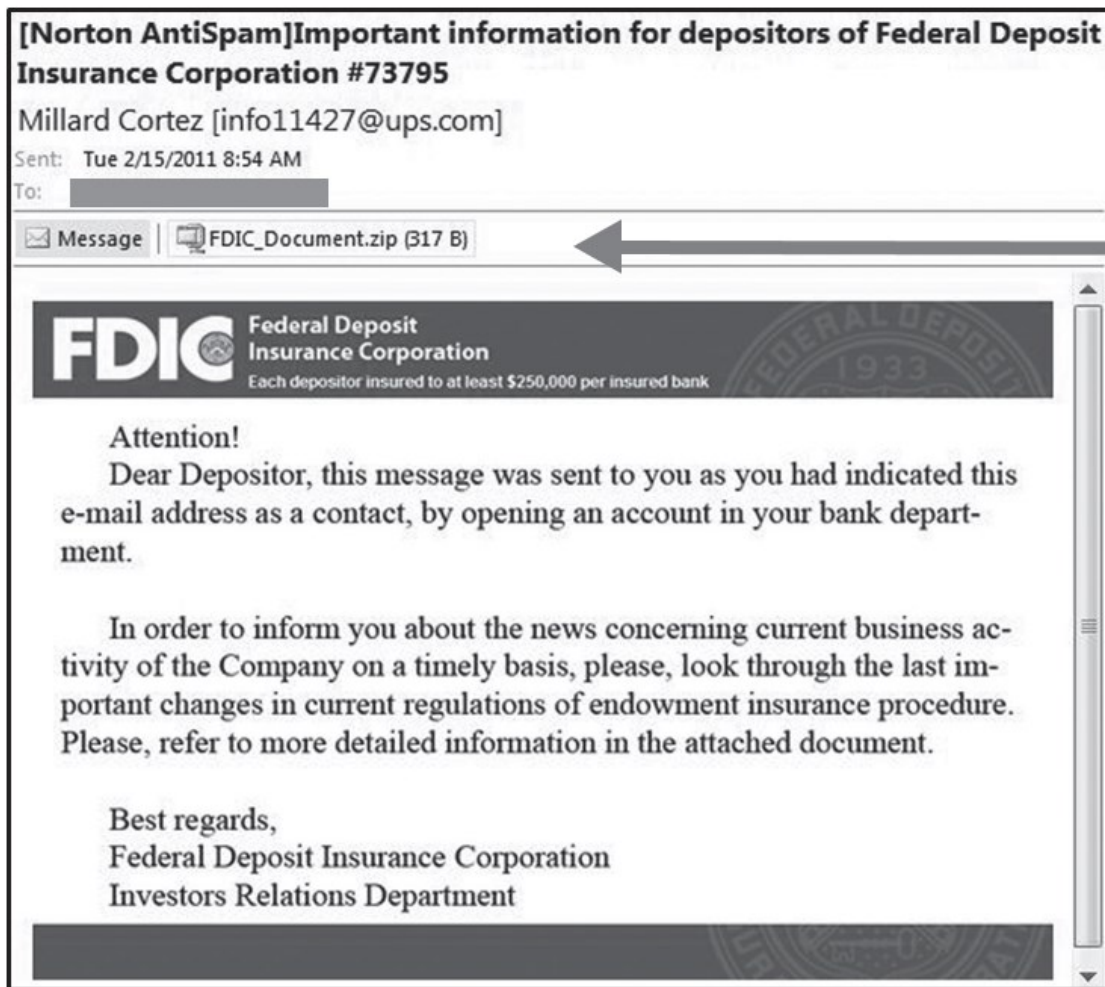
### Phishing Explored and Explained

question may be graphics images, sound or video files, or HTML and other plain-text files. Even an encrypted file may use steganography, so that its secrets still lurk inside the content, even when encrypted content is successfully decrypted. A person needs special software to embed hidden information in a file, but the software is readily available. Many download sites offer usable and free steganography packages.

Unpacking steganographic content also requires software. Such software parses the altered file to pick out all the secret bits hidden inside its normal contents. Once unpacked, that content may be used in a variety of ways: to provide information, pass secrets, or even to run a program, possibly malware, that might have been disguised inside the carrier file.

### ***The Second Surprise: A Malicious Attachment***

The second surprise in the message is the attachment, as shown in Microsoft Outlook (see Figure 16). You can see that the ZIP file is only 317 bytes. Inspection of the ZIP file shows only a single empty directory named FDIC Document, with no further content. Somewhere along the way, as the message made its way from its origination in Russia to the spam-filtering service in Seattle, Washington, someone or something stripped out its possible malicious content.



*Figure 16 Outlook shows that this message comes with an attached ZIP file*

The spam-filtering service used in this example—Spam Arrest—might have removed a suspicious or recognizable malware file. Or automated screening at some other **Simple Mail Transfer Protocol** (SMTP) server might have done it sooner.

If this message had arrived the way its builders intended it to arrive, here's what would have happened:

1. The recipient would have opened the ZIP file to read the fake FDIC document in it.
2. That document would probably have contained a macro or some other active content that would have unpacked the steganographic content from the FDIC image. This content may have been the keylogger/backdoor Trojan combination that is typical of phishing attacks.

## Chapter 4

### Phishing Explored and Explained

3. The software would have taken up silent and stealthy residence on the recipient's PC, harvesting keystrokes and sending them to a rogue server somewhere on the internet in a few days or a week.

### ***Telltale Signs in a Sophisticated Attack***

Even the fairly well-polished attack we've been discussing has some telltale signs that should alert cautious readers that this email is neither legitimate nor trustworthy.

First, who is Millard Cortez, and why is he sending an email about FDIC regulation changes? It's also odd that the email address is so generic (info11427) and comes from the ups.com domain. This is a blunder from the senders, who should have spoofed some official address at fdic.gov.

Also, the message content addresses a generic recipient ("Dear Depositor") rather than an individual person—which is a strong sign of phishing. It's easier and faster to use a one-size-fits-all salutation than to do the work necessary to personalize each outgoing message. The entire message is overly stilted and formal and includes some small signs of originating from someone who is not a native speaker of English. In particular, the phrases "of endowment insurance procedure" (missing a "the"), the extra comma after the word "Please," and "Investors Relations" (should be Investor Relations) are all a little off kilter.

The actual message header for this email, however, really shows the true colors and origins of the message. Figure 17 shows a text snippet from the SMTP transmission chain.

The supposed sending address for the message is 21.119.80.244, which is an arm of the U.S. Department of Defense in Ohio. However, the actual sending address is 95.78.99.252, which turns out to be in the city of Naberezhnye Chelny in Tatarstan, one of the member states in the Russian Federation. This isn't a terribly likely point of origin for a message from the FDIC, is it?

```
Received: from dynamicip-99-78-95-252.pppoe.chelny.ertelecom.ru (un-
known [95.78.99.252])
  by mx2.spamarrest.com (Postfix) with ESMTP id 16A28C84E88
  for <ignatz@spamarrest.com>; Tue, 15 Feb 2011 08:54:11 -0600 (CST)
Received: from [21.119.80.244] (helo=wsspcniyhnbna.mfxfumcptnbazx.ru)
  by dynamicip-99-78-95-252.pppoe.chelny.ertelecom.ru with esmtpa
  (Exim 4.69)
```

***Figure 17 Part of the message header of the FDIC phishing email***

## Attack Anatomy 3: Fake File Attachment

In this style of phishing attack, it appears there is an attachment delivered with the email message. If you hover your cursor over the attachment, as seen in Figure 18, the browser shows the so-called attachment is actually an image with a link to a website. Clicking this link will bring up a page in the browser which then proceeds as a standard phishing attack. Images with links pretending to be file attachments are always malicious.

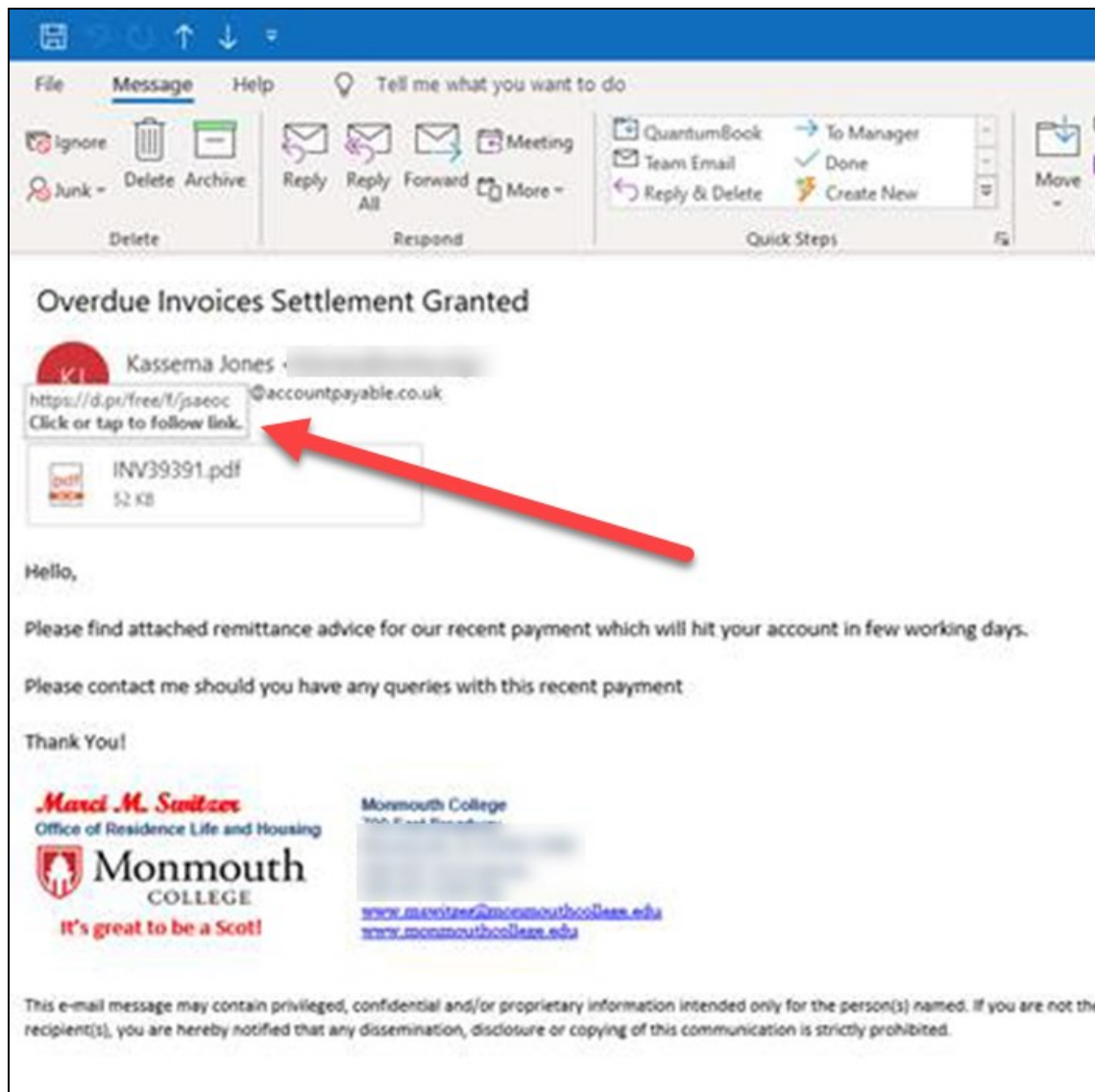


Figure 18 Fake file attachment image phish example

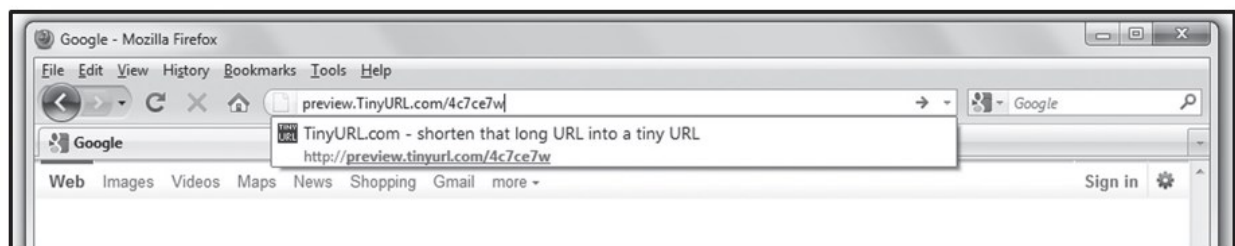
## URL Shortening: The Good and Bad

**URL shortening services** reduce the size and complexity of longer web uniform resource locators (URLs) by replacing longer links with a shorter link which then redirects to the eventual, longer, more complex, link. This is important in services such as Twitter, which limits tweets to 280 characters (the original the limit was 140 characters long). A single normal URL can easily consume most or all those characters crowding out any potential related message text. In addition, long, complex URLs are not only difficult to remember, they're also challenging to enter manually (as when copying one from a hard-copy book or an article). Shortening services use a redirect service that provides a shorter replacement—usually under 20 characters long—for a long original URL.

*Examples of services that provide shortened URLs are goo.gl, bit.ly, and TinyURL.com.*

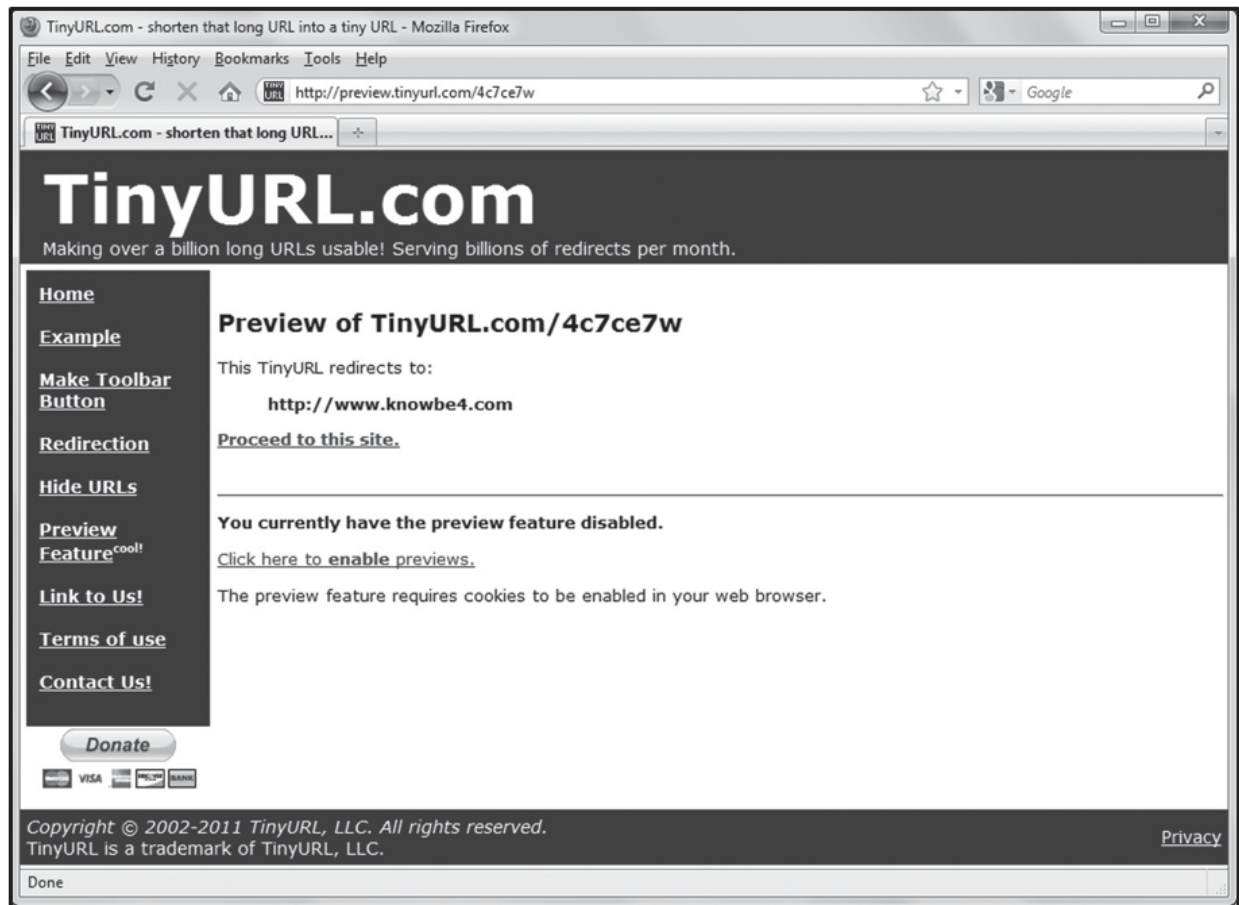
So far, URL shortening sounds like it's all good, but it can also be used by hackers to disguise rogue URLs and prevent easy detection of known malicious sites or destinations. For example, instead of seeing an obvious URL that indicates a website in Romania, the Ukraine, or Russia, a shortened URL link doesn't tell users much about where a link will take them or what they'll find when they get there. Phishing attackers love this!

Organization managers and IT personnel should warn employees to be wary when presented with shortened or abbreviated URLs. Most reputable shortening services offer preview options to show a fully expanded URL upon request, but the user must go out of their way to request the longer URL preview. For example, you can install a preview plug-in for the Mozilla Firefox web browser that presents previews for any *bit.ly* link. You can preview TinyURL links by typing preview in front of a link string. For example, to preview *TinyURL.com/4c7ce7w*, you'd type preview. *TinyURL.com/4c7ce7w* (see Figure 19). TinyURL tells you that this shortened URL redirects to our own website, at *www.knowbe4.com* (see Figure 20).



**Figure 19** *Previewing a shortened URL in Firefox*





**Figure 20** *TinyURL indicates that the shortened URL is linked to the KnowBe4 website*

## Social Engineering Red Flags

Social engineering is the attempt to deceive people into performing an action or divulging information against their own interests. Movies such as *Hackers* and *Wargames* contain excellent scenes that demonstrate social engineering by hackers pretending to be someone they are not in a believable fashion. In these movies, the hackers talk a worker, security guard, or even a receptionist, into giving them what they want. Social engineering is a con game.

Social engineering is a mind game. Social engineers play with human psychology to gain confidence and win confidential information. Cyberthieves use social engineering to realize several rewards: identity theft, financial fraud, or unauthorized access to protected systems.

Cyberthieves can apply manipulation techniques to many forms of communication because the underlying principles remain constant, regardless of the medium: Lure victims with bait and then

## Chapter 4

### Phishing Explored and Explained

catch them with hooks. Although most phishing attacks happen over computer networks, scammers are quick to target alternate channels. The same phishing principles apply whether an attack is via computer or by phone.

For emails and SMS messages, social engineering is done by making the message look like it came from a person or business that you trust. They can be quite convincing. Some of these messages are copied directly from official messages sent out by financial institutions or other organizations, making them very difficult to spot unless you know what to look for.

Most phishing messages contain red flags that help you identify them as attempts to social engineer. These red flags are described in the document: [Social Engineering Red Flags](#) (see Figure 21). You can download a PDF copy at <https://www.knowbe4.com/hubfs/Social-Engineering-Red-Flags.pdf>.

# Social Engineering Red Flags

- FROM**
  - I don't recognize the sender's email address as someone I **ordinarily communicate with**.
  - This email is from **someone outside my organization and it's not related to my job responsibilities**.
  - This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
  - Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
  - I **don't know the sender personally** and they **were not vouched for** by someone I trust.
  - I **don't have a business relationship** nor any past communications with the sender.
  - This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.
- DATE**
  - Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?
- SUBJECT**
  - Did I get an email with a subject line that is **irrelevant or does not match** the message content?
  - Is the email message a reply to something I **never sent or requested**?
- ATTACHMENTS**
  - The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
  - I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.
- CONTENT**
  - Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
  - Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
  - Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
  - Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
  - Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?
- TO**
  - I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
  - I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.
- HYPERLINKS**
  - I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
  - I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
  - I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofarnerica.com](http://www.bankofarnerica.com) — the "m" is really two characters — "r" and "n."

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

KnowBe4  
Human error. Conquered.

Figure 21 Social Engineering Red Flags



## *Surefire Ways to Avoid Phishing*

First and foremost, the best ways to avoid falling prey to phishing attacks are to ignore spam and to steer clear of clicking links in tweets, Facebook pages, suspicious blog posts, and the like. If that's too much to ask, be sure to look over messages, tweets, and posts carefully, looking for the telltale signs of phishing discussed in this chapter. Above all, never respond to questionable emails or click the links in tweets and posts. If you have a concern about an account or a financial transaction, directly visit the home page for your institution (not by clicking any link). Then either check your account online or use the organization's contact information to reach out to them by email or phone. If you initiate a conversation, that's one way to be sure scammers aren't involved!

## *What Criminals Want from Victims*

Though phishing can happen in various ways, the information that is stolen is typically numeric. The most valuable information includes the following:

From individuals:

- ✓ Credit card details
- ✓ Account numbers and personal identification numbers (PINs)
- ✓ Social security numbers
- ✓ Passport numbers
- ✓ Usernames and passwords
- ✓ Birthdays and anniversaries

From businesses:

- ✓ Insider information
- ✓ Trade secrets
- ✓ Hijacking systems
- ✓ Sabotaging the business
- ✓ Leaking information
- ✓ Passwords to accounts with high privileges
- ✓ Theft of databases
- ✓ Holding data ransom
- ✓ Denial of service
- ✓ Names and information about management

Criminals use the data they harvest for identity theft and other forms of fraud. Knowing birth dates and anniversaries can help them crack passwords or challenge response sequences

## Chapter 4

### Phishing Explored and Explained

(questions) that sometimes serve as forms of **authentication**, which is the process of identity verification.

## *How Criminals Lure Victims*

The fishing bait-and-hook analogy applies well to phishing. Scammers lure victims by using bait that targets specific social, mental, or emotional triggers. The phishing “lures” cybercriminals use to bait victims can take many forms, including the following:

- ✓ **Account suspension:** Threatening to suspend account access
- ✓ **Billing verification:** Requesting confirmation of or updated billing information, which is actually not needed
- ✓ **Unauthorized sign-in:** Warning that an account is locked because the number of attempts to log in exceeded a threshold
- ✓ **Software downloads:** Offering a free utility that will fix a computer problem
- ✓ **Lottery prizes:** Offering bogus winnings with processing fees

## *How Criminals Profit from Data Theft*

Phishing is rarely a one-act crime. Usually, it begins as a broader criminal strategy that involves various illegal activities, including stealing, selling, and otherwise misusing private or confidential information. A criminal who obtains social security numbers might obtain credit in the victims' names, buy goods online with that credit, and then sell those goods online or overseas. In the case of healthcare fraud, criminals may even sell stolen patient data to organizations that in turn use the data to defraud Medicaid and Medicare.

Criminals benefit from stolen information in the following ways:

- ✓ Using stolen identities for monetary gain
- ✓ Controlling the financial accounts of others
- ✓ Purchasing products and services
- ✓ Submitting phony credit and loan applications
- ✓ Filing for fraudulent tax refunds
- ✓ Pilfering funds, stocks, or securities
- ✓ Laundering ill-gotten money
- ✓ Stealing government benefits, such as social security checks and unemployment benefits

\*\*\*

In many cases, committing the crime is easier than the what the victims face cleaning up the consequences. Criminals need only a few pieces of vital information and a little time to defraud entire groups of people at once. Victims, both individuals and companies, can spend years recovering from the damaging effects of crimes. It's no wonder criminals see phishing—and the variants we're about to discuss—as easy-entry, low-risk crimes that yield high financial returns.



# Chapter 5

## Variations on the Phishing Theme: Smishing and Vishing

Phishing tricks victims, whether at home or in the workplace, into revealing private or sensitive data to an unknown party or into performing actions against the victim's own interests. Phishing attempts to fool victims into acting on bogus requests for personal, organizational, or private data that only authorized parties should know. Typical phishing attacks occur over email and instant messages, but what began as computer fraud now also targets mobile phones and other wireless devices.

Because phishing is a form of social engineering, scammers try to appeal to a victim's sense of greed or fear, obedience to authority, social pressures, or trust in strangers. Phishing is an issue that affects people rather than technology, and it's unreasonable to expect software solutions to prevent all phishing attacks. Just as a weak password undermines the strongest authentication mechanism, uninformed choices undermine an individual's safety against social engineering.

Phishing has many derivatives and variations. In this chapter, we focus primarily on two interrelated types of phishing: smishing and **vishing**.

### *Anatomy of a Smishing Attack*

**Smishing** is phishing conducted via Short Message Service (SMS), a telephone-based text messaging service. A smishing text provides bait that attempts to entice a victim into revealing personal information or performing a harmful action; in this case, the hook is usually a uniform resource locator (URL) or a phone number. Attacks of this kind show scammers' versatility in reaching out to ensnare victims across different types of media.

For example, say that a credit union member receives a text message, warning that the member's account has been compromised and instructing the member to call a toll-free number. When the person calls the number, an automated system asks the person to enter his or her account number, PIN, password, or other private information. The criminal then uses this stolen information to perform identity theft. As another example of smishing, a text may urge users to install mobile antivirus software. When the person installs the software, he or she actually installs malware instead.

## Chapter 5

### Variations on the Phishing Theme: Smishing and Vishing

As discussed earlier, phishing draws on principles from social engineering. Those principles also apply to different media, including smishing. The strategy involved in smishing is ancient—it's just another form of Trojan trickery—but the delivery method is modern. Complex smishing attacks work in two stages to bait victims via phone message and hook them via computer. Smishing may employ Trojan software or request private data to hook victims. Either way, the delivery methods remain the same.

*You may see smishing written as SMiShing to tie the term more closely to SMS.*

### **Selecting the Bait**

Bait texts create a false sense of urgency to encourage a victim to take action. Basic examples include unknown service charges, phony online purchases, cash prize winnings, and suspended account reactivation.

### **Setting the Hook**

A smishing hook tries to entrap victims through solicitation and capture of sensitive information, or installation of malicious software. Hooks needn't be clever or complex to be effective. A person receives a text message that prompts an action. To gather information, the criminal might use dial-tone interpreters to decipher dial pad input, or speech interpreters to analyze speech. The action the victim takes usually involves the installation of a Trojan program.

### **A Smishing Example**

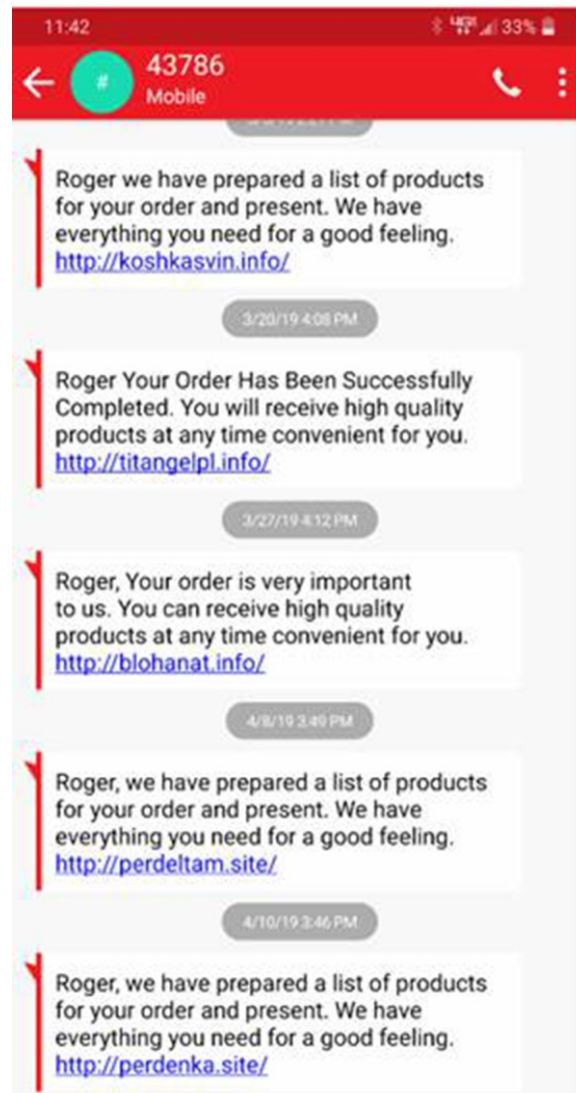
Let's examine an example of a smishing attack:

1. The thief establishes a range of numbers to autodial. Even if only 1% of 1,000 people respond, the thief stands to gain quite a lot.
2. The thief creates a link to download fictitious security software. Once the hook is set, bait will lure the victims.
3. The thief sends a text message to a victim. The text pretends to be from the victim's phone company and falsely declares that their phone has been detected as harboring a phone virus and that if it isn't removed immediately, they will cut off the service. The text urgently instructs the victim to download "necessary" security software.
4. The victim receives and reads the text message. The text message (bait) lures the victim to bite on the hook.
5. The victim complies with the instructions in the text message. The victim dials the callback number, installs the requested software, and is "hooked."

This attack could easily lead the victim to reveal private data to an automated system.

## Variations on the Phishing Theme: Smishing and Vishing

As shown in Figure 22, this smishing scam looks like it came from a shopping website. The scammer wants you to click on the link, which can either go to a scammer website or download malicious software to your smartphone. Everything about this text message—from content (a list of products) to structure (no SMS or email opt-out) to delivery (unsolicited message)—is questionable. They depend on someone clicking the link just to find out about the products or the so-called order. A trusting person with little security awareness may think nothing of clicking the link.



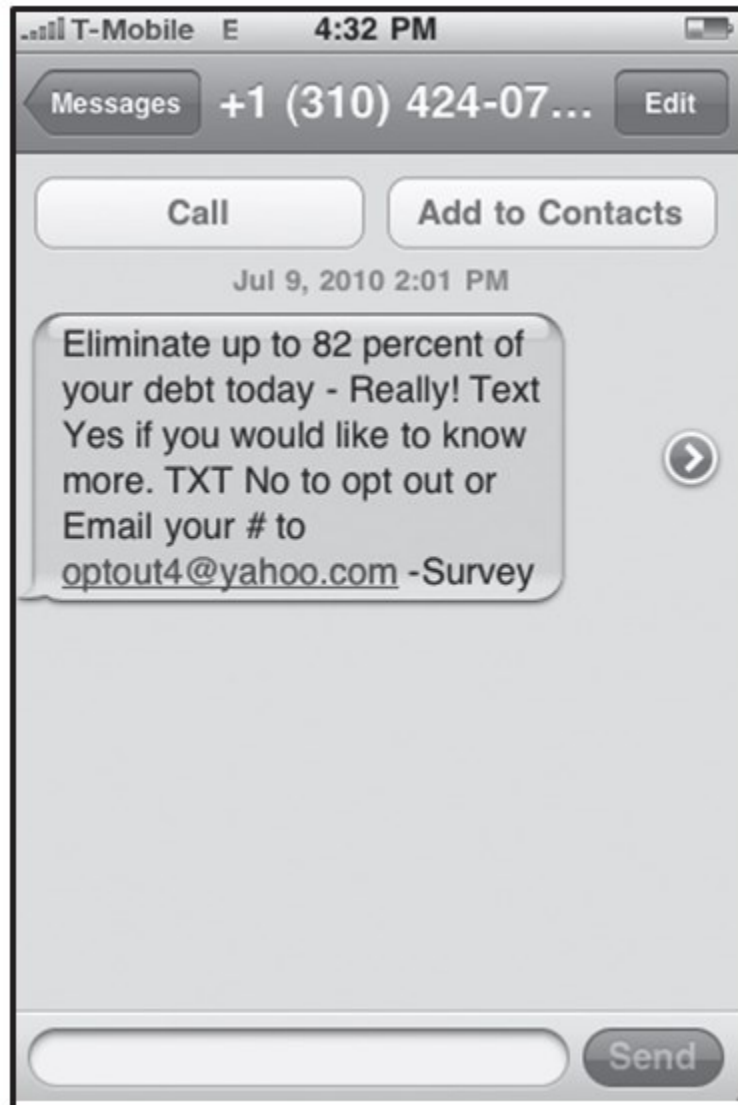
**Figure 22** Example smishing attempt

Obvious attempts are easy to spot and avoid. Bad grammar, poor spelling, unsolicited messages, bogus URLs, forged emails, and shady get-rich-quick schemes are typical attempts. A well-crafted text at the right time can fool almost anyone. Anxiety, stress, fear, anger—emotions that erode

## Chapter 5

### Variations on the Phishing Theme: Smishing and Vishing

our ability to think clearly and judge correctly—are excellent triggers for a scammer to exploit. Other times they are just appeals for a person to easily save money on their bills (as shown below).



*Figure 23 A blatant smishing attempt aimed at hooking people with debt problems*



## *Anatomy of a Vishing Attack*

Vishing is a phishing attack conducted by telephone, usually targeting anyone with a phone, including **VoIP** (Voice over Internet Protocol) services, like Skype and Zoom. Vishing exploits public trust in landline telephone services and is difficult for authorities to monitor and track. Scammers can fake caller ID data and hide behind bill-payer anonymity to dupe victims.

The popularity of vishing attacks has risen. Commercial and residential VoIP users are not required to provide valid caller ID data, which makes this technology ideal for committing fraud. Potential consequences of vishing include eavesdropping, unauthorized access to voicemail or billing information, voicemail overloading, and phone number harvesting.



### **Voicemail Overloading and Phone Number Harvesting**

**Voicemail overloading** is also referred to as spamming over internet telephony. Much like getting spam email, a user can get junk voicemails. Spammers simply send a voicemail message to thousands of IP addresses at a time. Because voicemail spamming is as easy as email spamming, a VoIP user can get a lot of junk voicemails quickly.

**Phone number harvesting** can occur many different ways, any method used by an attacker to collect a valid phone number, to which they can then send unwanted calls and messages. Here are some example collection methods:

- Numbers are collected when a user downloads “free” ring tones which require a phone number to download.
- User responds to a spam text message, which replies with their phone number.
- **Number harvesting** also describes a VoIP attack in which an attacker monitors incoming and outgoing calls on a VoIP system they have broken into.

## *Selecting the Bait*

Thieves may employ several phishing strategies to bait victims. All the emotional appeals, sense of urgency, and timing work exactly the same way as in other forms of phishing. What changes is mostly the delivery: In the case of vishing, voice-based telephony is the delivery system.

## *Setting the Hook*

Vishing hooks may use callback numbers and automated recordings. Victims take the bait, dial the callback number, listen to the recording, and reveal sensitive information. Large-scale operations may employ an answering service or a call center unwittingly participating in the

## Chapter 5

### Variations on the Phishing Theme: Smishing and Vishing

fraud. Hooking victims through vishing is nearly identical to hooking them in other forms of phishing; it's mainly the delivery mechanism that's different.

## *A Vishing Example*

Let's examine an example of a vishing attack:

1. The thief uses a list of numbers stolen from a financial institution, a war-dialer to automatically call numbers, and a legitimate voice messaging service. The spoofed caller ID shows a legitimate organization name.
2. An automated recording alerts the consumer to the bait. The recording urges the victim to call a fake number for one of a variety of reasons, such as account expired, account overdrawn, fraudulent activity, billing errors, or whatever suits the scam.
3. The victim dials the provided number, which plays an automated recording. Voice instructions direct the victim to provide credit card or account numbers.
4. The thief captures any other necessary details, such as security PINs, expiration dates, date of birth, and other important information.

In real world examples, residents of Elgin, Texas, received automated calls from fraudsters claiming to represent KCT Credit Union and First Community Bank. In New York, recordings claimed to represent Cattaraugus County Bank and Mt. Vernon Money Management. In vishing attacks, sometimes the banks and credit unions are identified by name. Sometimes the callers pose as travel agents or lottery officials for unknown agencies. In every case, these callers offer only lies and deceit.

Other popular scams include:

- ✓ The fake Microsoft tech support scam, in which the victim gets an unsolicited call from a scammer pretending to be a Microsoft tech support person calling to proactively help the victim with a purported malware infection.
- ✓ Fake IRS or police payment scams, in which the scammer tries to scare the victim about a fine or payment that is long overdue. They often threaten to send the police or take some other extreme action.
- ✓ Calls to grandparents saying a grandchild is in trouble with the police and they need to send money without getting his parents involved.

All these scams rely on the victim trusting that the caller is telling the truth about the supposed problem or crisis. The best thing to do is to simply hang up on the caller. If they continue to call back, most smartphones give you the option to block specific phone numbers. Persistent scam callers should be reported to the phone company or law enforcement.

## **WARNING!**

*Vishing isn't limited to VoIP services with user-specified prefixes and identification. Third-party companies offer phone spoofing services, allowing callers to pay for anonymity. Some services provide VoIP for private branch exchange (PBX) systems, which connect the internal telephones of a private organization. These services also allow companies to select arbitrary phone numbers, and thieves use this situation to their advantage.*

## *Why Smishing and Vishing Works*

Vishing works because of technology convergence—that is, the merger of formerly separate and distinct technologies. Systems that were once isolated from each other can now interact with each other. Broadband phone services send calls over computer networks. The connection points to older phone networks create openings for criminals to commit phone fraud.

Another reason vishing and smishing are successful is the lack of good authentication. The phone number or caller ID, for example, can be easily changed by hackers to be anything they want, displaying the number and name of a bank or the IRS office.

Broadband phone services allow users to acquire phone numbers with area codes in remote cities. Distant criminals in other countries can create the illusion of calling from local organizations. In some cases, intruders find ways around network defenses and actually do make calls from legitimate organizations. Proprietary VoIP protocols only worsen the problem by making it difficult for security experts to combat VoIP vishing.

Several other factors contribute to the success of vishing:

- ✓ Inherent trust placed in telephone systems, especially compared to internet messaging
- ✓ A reachable phone-using population
- ✓ General acceptance of automated phone systems
- ✓ Common usage of overseas call centers with foreign callers
- ✓ Flexibility of voice and text recognition
- ✓ Tailored phone calls that seem more personal to the victim

## Chapter 5

### Variations on the Phishing Theme: Smishing and Vishing

IP telephony creates the opportunity for vishing attacks because of its social and technological reach. VoIP allows criminals to reach anyone, from any location in the world. Sending, receiving, and automating calls, as well as routing traffic through proxies involves minimal cost. Advanced vishing may use a malware agent to handle message delivery. An example of a malware agent is a **botnet**, which is a network of remotely controlled computers, usually meant for malicious purposes. (You'll learn about botnets in Chapter 10.)

## *Other Possible Variations Surely Lie Ahead*

People buy hundreds of millions of smartphones every year, creating a rich market for scammers. As criminals turn to using text messages and VoIP to target victims, we can expect to see more fraud both at home and at work. We will see more worm, virus, spam, and smishing attacks against mobile users via SMS, mobile internet, Bluetooth, and Wi-Fi.

The following are a few of the emerging or increasing methods of smishing or vishing:

- ✓ **Mobile banking fraud:** As more people use their mobile phones to access online banking, fraudsters will target them with more realistic text messages that look like they're from the bank or credit union.
- ✓ **Mobile email downloads:** People increasingly access their email accounts using smartphones, making it easier for thieves to download malicious software to phones. Most phones don't have antivirus protection like PCs do, so detection is much more difficult for the user.
- ✓ **Fake access points (APs):** Bogus Wi-Fi networks look like legitimate shared hotspots in public places (such as airports, coffee shops, and hotels). When users log in or use these access points from their PCs or mobile phones, criminals capture all their data.

With new technologies rolling out every day, and as criminals' experiment with these technologies, we will continue to see smishing and vishing scams adapt as well.

## *Avoidance Techniques to Live By*

Because cellphone users are subject to smishing, mobile carriers must continually adapt their defenses to filter suspicious SMS texts, much like internet service providers filter spam email. There's currently little recourse against many vishing scams, which may involve a single caller or an entire call center.

Common sense is a general best practice and should be an individual's first line of defense against online or phone fraud. Unfortunately, this is not always simple or obvious. Therefore, awareness training is a necessary line of defense against all online privacy and security threats.

## Chapter 5

### Variations on the Phishing Theme: Smishing and Vishing

Basic safety tips and best practices include the following:

- ✓ **Trust no one:** Even if you think a call or text originated from a legitimate institution, question the credibility of the source.
- ✓ **Remember caller ID can be faked:** Anyone can set their phone's caller ID to anything they want.
- ✓ **Know your numbers:** Call only trusted numbers, like those printed on billing statements or posted on official sites.
- ✓ **Hang up on uninformed callers:** Any caller representing a legitimate organization should know their customers and who they're calling, so hang up if asked for private or sensitive information that they should already know.
- ✓ **Ignore and flag suspicious texts:** Any unexpected text requesting an action should be regarded as suspicious unless proven legitimate using other methods.
- ✓ **Watch out for bogus pop-ups:** At a real site, a fake pop-up window may request sensitive information and appear to be part of the legitimate site. Use pop-up blockers to stop pop-ups from appearing in the first place.
- ✓ **Reveal nothing, conceal everything:** Provide no useful information to random callers. In fact, be cautious about revealing personal information to any caller. If you're asked for private or confidential information, insist on calling the company back using a number you know is legitimate.
- ✓ **Verify and validate:** If you receive an alert about account abuse or suspension, call the company directly and inquire about your account. Never use any contact number provided in an alert and always look up actual service numbers from bills or authentic websites.

As with any other online threat, with the various types of phishing, exercise good judgment. When it comes to fraud, you can never be too untrusting. Exercising too much trust is a weakness that creates victims out of just about anyone.

\*\*\*

Cybercriminals will take advantage of any perceived weakness they can find using every possible device and attack vector. The rule of thumb to follow is if a computer or smart device can access the outside world it's vulnerable to attack.



# Chapter 6

## Targeted Scams: Spear Phishing, Whaling, and More

A great many phishing attacks look and feel much like ordinary spam. Emails, tweets, and social network posts go out in volume. They simply target the general public—or at least anyone who actually reads the communication that starts the attack.

Not all phishing attacks are scatter-shot in their approach, however. Certain types of phishing schemes have quite a bit of focus. The attackers research a target population or a set of targets. These phishing attacks may not be as specific as wire and insurance frauds in the mid-twentieth century, but the attacks target specific types of individuals—and sometimes even particular persons by email address. The more focused a phishing attack, the more work is involved for the attacker. However, payoff is larger. According to the SANS Institute, spear phishing attacks are successful 95% of the time when the target is an enterprise network. [18]

The benefits of a targeted attack can be more substantial than fleecing the general public. In targeted phishing attacks, cybercrooks are likely to target victims who are better-heeled than the general populace. A successful targeted phish is likely to produce more cash or other items of value for the extra effort involved.

When it comes to targeted phishing attacks, security experts distinguish between two types of attacks: spear phishing and **whaling**. Whereas spear phishing goes after specific types of targets, often by organizational affiliation, whaling goes after specific (usually substantial and presumably wealthy) targets by position, identity, or name.



### Spear Phishing and Whaling

General phishing can attack target populations with specific types of accounts. These might be individuals with Yahoo or Gmail email accounts or individuals who bank at Wells Fargo or Citibank. **Spear phishing** uses information about and targets a specific organization or company. Spear phishing messages may appear to originate from a large or a business acquaintance, colleague, business partner, or vendor. Sometimes in more customized attacks, messages that hit a user's inbox appear to come from a coworker or a member of the management team at the victim's own company.

Just as old-fashioned, seaborne whaling targeted the Leviathans of the deep, today's whaling attacks target high-ranking executives at major organizations or other highly

## Chapter 6

### Targeted Scams: Spear Phishing, Whaling, and More

visible public figures. These attacks are carefully aimed at specific individuals with greater power and influence at an organization or able to perform specific actions that result in greater gains if the phisher is successful. They feature all the details that legitimate email would also include. But because whaling is a kind of phishing attack, whaling messages create a sense of urgency or a need to respond to their sender. They also provide a handy link for recipients to click. Once on a phishing site, victims are subject to drive-by downloads.

Let's take a look at the mechanisms of spear phishing and whaling attacks.

## *Spear Phishing Attacks*

Spear phishing attacks usually exploit publicly accessible company websites that offer contact information for employees and information about the target company or organization. Using details available from news stories, press releases, LinkedIn, and other sources, an attacker crafts an email message. This message appears to originate from someone inside the organization who has a right to ask for confidential information. It might be an HR person, a system administrator, a superior officer, or a first- or second-level manager in another department.

Spear phishers usually request usernames and passwords or ask victims to click a link that secretly installs drive-by downloads on their PCs. If one employee falls for this ploy, a spear phisher can impersonate that victim and start working his way up the food chain at the target organization. Ultimately, the spear phisher may hit pay dirt and obtain administrative passwords, bank account information, access to intellectual property, other valuable data, or be successful in getting someone inside a specific organization to run a malicious malware program.

The successes in spear phishing result from the organizational knowledge and details that attackers use to make themselves appear to be known and trustworthy. Information in a spear phishing message looks legitimate, and the request seems valid. The recipients who fall for the ruse provide the requested details or visit the phishing site and can fall prey to drive-by downloads.

Here's a dramatic example of successful spear phishing, as reported at [educause.edu](http://educause.edu) by security expert Aaron Ferguson. A person identified as "Colonel Robert Melville" who had a West Point email address sent out a spear phishing message to cadets at West Point; 80% of them responded to this email. At West Point, the prevailing email culture is that any message that includes the rank COL (a military abbreviation for the rank "Colonel") in the salutation requires immediate attention. If such an email includes instructions or orders, cadets are to act upon them as directed. This particular email was a test rather than a real phishing attack, but it deliberately sought to exploit cadet culture, mindset, and training. In fact, this email was actually sent by the West Point U.S. Military Academy (USMA) Computer Emergency Response Team (CERT).



According to Ferguson, the exercise tested the “security posture of the institution” and helped determine “the effectiveness of current security awareness, education, and training.”

Students who clicked the link in the message were notified that they had been duped. They were also warned that their response could have resulted in the download of malware to their PCs. Given the high intelligence and caliber of the West Point Corps of Cadets, this example illustrates that well-crafted spear phishing attacks can produce a higher-than-normal response rate. Whereas a typical rate seems to be one in five, this experiment produced a four-in-five response rate.

## Whaling Attacks

The *New York Times*, in 2008, [19] reported for the first time about an attack that targeted thousands of high-ranking executives at financial services companies around the country. Each person received an email message presented as a subpoena from the U.S. District Court in San Diego, California. Each message included the executive’s name, company, address, and phone number and instructed its recipient to appear before a grand jury in an upcoming civil trial.

The handy message link in this case supposedly led recipients to a complete copy of the subpoena. But recipients who followed that link were subject to a drive-by download that included a keylogger and a backdoor Trojan. The *Times* story reported that “less than 40 percent of commercial antivirus programs were able to recognize and intercept the attack.”

The particular attack reported in the *Times* was pervasive enough that two separate California federal courts, as well as the administrative offices of the U.S. courts, posted warnings on their websites. The attack prompted hundreds of calls daily to the courts identified. At the same time, antispam company MX Logic reported that it was observing 30 or more messages per hour matching this attack. More disturbingly, more than 2,000 victim PCs showed attack signatures indicating that the malware download had infected the target machines.

According to subsequent analysis of the attack profile and the malware involved, security experts linked this attack to an earlier assault that occurred the year before. In that case, the email message supposedly originated from the U.S. Department of Justice and informed the recipient that a suit had been filed against his or her company.

Software installed on victim machines communicated with a server in Singapore. The originator of the email appeared to have substantial knowledge about the workings and operations of the financial services industry in general. Various subtle clues in the message, however, suggested that the attackers were not intimately acquainted with the U.S. court system. Other clues pointed to “Britishisms”, suggesting that the attackers might be based in Hong Kong or nearby in China.

## Chapter 6

### Targeted Scams: Spear Phishing, Whaling, and More

This was a very carefully constructed and well-thought-out attack. But if the targeted executives had stopped to think, they would have immediately recognized it as a ruse. Why? Because a subpoena is an official court document. To be successfully delivered, a subpoena must be properly served. This requires filing a subpoena form, notarizing the subpoena, preparing and filing an affidavit of service, and delivering the documentation to a designated recipient in person. If necessary, a subpoena's server may be called upon to testify in court that the subpoena was served and to attest that all serving requirements were met. Email delivery is not an acceptable way to serve a subpoena!

Whaling attacks are often quite sophisticated. SMX, a computer security firm, described a 2015 attack in its blog [20] that targeted the CFO of a large company in New Zealand. The CFO received an email which was apparently sent by the CEO (who was out of the office), ordering him to transfer \$192,000 to a bank account located out of the country to pay for supplies. The email appeared to be valid, with the CEO's correct name and email address, and contained no malicious links or attachments, which meant it was not stopped by any filters.

The scammers purchased the domain name that appeared similar to one used by the firm mentioned in their email. The CFO replied to the message, and scammers used that domain to continue the email exchange. Several messages went back and forth from the CFO to the scammers because the amount requested was larger than normal and bypassed the standard procedure of requiring a purchase order.

This scam almost worked because the CEO had an iPad and the CFO knew he was out of town during that time. It was not unremarkable to receive messages of this nature from the CEO, and the only reason the scam failed was the amount was relatively large. This prompted the CFO to question the request.

Many whaling attacks are successful. Pathé, a Dutch film company, fell victim to a BEC scam that cost them about \$21 million. The scammers spoofed the email address of the CEO of the company and claimed they were in acquisition talks with a company in Dubai. They needed a payment of almost a million dollars and said this would be a loan to be repaid quickly. The payment was approved by the finance boss, and three more payments were made. The headquarters in Paris figured out what was happening, fired two executives, and the scam ended. [21]

Another firm, this time an Austrian aerospace manufacturer, lost roughly \$55 million to a classic whaling attack. A scammer pretended to be the CEO and successfully convinced a finance department employee to initiate a money transfer of the funds. [22]

## *Social Engineering Redux: Upping the Ante*

The apparent validity and urgency of the request coming from a trusted person along with the higher potential damages makes spear phishing and whaling more dangerous than a regular

phishing attempt. A regular phish may scam someone out of hundreds or thousands of dollars. A spear phish or whaling attempt may get tens of millions of dollars. Spear phishing attacks appear to come from trusted or well-known business partners, colleagues, or coworkers. Whaling attacks often appear to originate from people or entities they know, such as financial, billing, legal, or banking contacts, they regularly work with.

The West Point cadet's example shows how "chain-of-command" expectations work both in corporations and within the military. In both instances, underlings feel compelled to respond quickly. It illustrates that messages that appear to come from higher up in one's own chain of command not only invite a response, but, in some sense, command one. You can also argue that the same logic applies to the New Zealand whaling attack, where executives' inclination to comply with court orders and instructions was exploited to elicit immediate response.

When they succeed, both spear phishing and whaling attacks are best understood as the triumph of social engineering over common sense. The plain fact is that clicking a link in an email message, in a tweet, or on a Facebook page invites trouble. This is true even when the invitation to click appears to originate from a trusted source. Only when users realize that clicking a link carries a certain risk will they stop and ask, "Should I click it or skip it?" In many cases, skipping it is the safest course of action. A quick check of the uniform resource locator (URL) may reveal a different-than-expected domain name, so that's a good habit to carefully examine and verify URLs in messages any time you think you might actually be interested in what's supposedly at stake, on offer, or of interest.

One scary aspect of the West Point cadet's example is that so many of the targeted recipients fell for this attack. We suspect that the same is true for other targeted phishing attacks. Certainly, the report in the *New York Times* that more than 2,000 executives' PCs were infected with malware from a single attack suggests a higher-than-normal success rate.

The secret to the success of a targeted phishing attack appears to come from knowledge of the victim's world and surroundings. What makes these attacks compelling is the phisher's understanding of authority figures or agencies that can incite response. As explained earlier, this is a case of ingrained behavior trumping common sense. If an attack presents a convincing imitation of the victim's world and provides a good reason to get people to click a link, the attack has a chance of succeeding.

## *Anatomy of a Whaling Attack*

The subpoena scam described earlier in this chapter is a good example of a well-crafted whaling attack. The scam message (see Figure 24) looks similar to a real subpoena (Figure 25). The originating email address, not shown here, includes an appropriate .gov domain. The link inside

## Chapter 6

### Targeted Scams: Spear Phishing, Whaling, and More

the message also looks legitimate, although a domain name lookup shows that it was registered in the United Kingdom, not in the United States.

AO 88(Rev.11/94) Subpoena in a Civil Case
UNITED STATES DISTRICT COURT
Issued to: XXXXXXXXXXXXXXXXXXXX
COMPANY NAME HERE
COMPANY PHONE NUMBER HERE
SUBPOENA IN A CIVIL CASE
Case number: 91-201-NKE
United States District Court
YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

***Figure 24 This mocked-up text from the whaling message described in this chapter looks somewhat like a real subpoena***

AO 88 (Rev. 07/10) Subpoena to Appear and Testify at a Hearing or Trial in a Civil Action

---

UNITED STATES DISTRICT COURT

for the

[Redacted]

[Redacted]

Plaintiff

v.

[Redacted]

Defendant

)

)

)

)

Civil Action No. [Redacted]

**SUBPOENA TO APPEAR AND TESTIFY  
AT A HEARING OR TRIAL IN A CIVIL ACTION**

To: [Redacted]

**YOU ARE COMMANDED** to appear in the United States district court at the time, date, and place set forth below to testify at a hearing or trial in this civil action. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

**Figure 25 A portion of a PDF of a subpoena downloaded from the U.S. Courts website**

Close attention to the differences between Figure 24 and Figure 25 shows that the cyberthieves in this whaling attack didn't bother to download the latest civil subpoena forms from the web, even though it was readily available online. There are obvious differences in layout and language. You can see the various "Britishisms" cited in the Times story in the words "hereby," the language "appear and testify," and in mention of a Grand Jury (not relevant to civil cases in U.S. courts).

However, for executives trained to respond quickly to court documents, this phishing attack was well constructed to elicit the response it sought: to get recipients to click the provided link. Though victims didn't see the full text of the subpoena, the drive-by download was already under way.

## Spotting an Attack

Phishing scams—including spear phishing and whaling attacks—end with a call to act, which usually means clicking a link or opening an attachment. As soon as you spot a link you're supposed to visit in an email, in an SMS message, in a tweet, or on a social network page, you should be suspicious. Although there may be plenty of good reasons to click links from parties you know and trust, responding to pleas, requests, or demands for immediate action is never advisable.

## Chapter 6

### Targeted Scams: Spear Phishing, Whaling, and More

Table 3 compares the different kinds of lures that phishing attacks float in front of their intended victims with how legitimate interactions and requests normally work.

***Table 3 Attack Lures Versus Legitimate Interactions***

<b>Attack Lure</b>	<b>Legitimate Interaction or Instruction</b>
Click the link, or your email is suspended	Visit our website and consult your My Account settings
Click the link and collect your winnings	Notification occurs by mail, often registered
Click the link to read the subpoena	Subpoenas are served exclusively on paper
Click the link, or your account is frozen	Visit our website or call our customer service department
Click the link to download your update	Visit our website and use our download page
Click the link and access your grades	Log in to your student account online and check your current transcript

Note that phishing messages can sometimes be exact, word-for-word copies of valid messages from vendors, complete with graphics, footnotes, and unsubscribe instructions. A best practice is to visit the website **WITHOUT** clicking the link in the message. Instead, type in the legitimate website URL into the browser yourself. For example, if the message demands you click a link to visit your bank's website, open up your web browser, and enter your bank's URL manually without referring to the one in the message.

## ***WARNING!***

*If using the phone is your preferred way to conduct business, get the phone number from the company website or an online directory, not from an email message.*

Some legitimate interactions, such as serving a subpoena, simply don't happen online. You might receive an email notification that you are to be issued a subpoena. But the subpoena itself will always be delivered in person, on paper, by a live human being. The same thing goes for sweepstakes, lottery, and contest winnings. While you may get a phone call, you will also be notified in writing for legal reasons. And when your winnings are delivered or deposited, you'll also get a written notification from the IRS!

## *Surefire Spear Phishing and Whaling Avoidance*

We've said it before, we'll say it again, and we're saying it now: Don't click a link in an email, in a tweet, or on a social networking web page without confirming that it's safe to do so (stop and think before you click). As the whaling attack details emphasize, clicking a link sometimes is all it takes to succumb to an attack. Usually, though, you'll be prompted to run a program (a trojan executable), open a file, or perform an action.

When cybercriminals take the time and expend the effort to mount a serious attack, the consequences can be serious. Think of the 2,000-plus PCs compromised by malware in the U.S. district court subpoena whaling scam. And think of the heavy internet traffic that was seeking to infect more CEOs. Can you appreciate the clear and present dangers involved in whaling?

If general, if you are asked to get involved with your account, don't click on the provided link unless you are absolutely sure it is legitimate. It's far safer to log into the legitimate vendor's website directly and then see if the same request is presented to you. If the request is real, the vendor will ask you about it when you log in. (Chapter 18 covers Transport Layer Security, or TLS, and shows examples of the padlock icon that indicates TLS is involved.)

## *CEO Fraud*

A new type of scam called CEO Fraud (the FBI calls it "**Business Email Compromise (BEC)**") is rapidly expanding. Taking into account international victims, the losses from BEC scams total more than 26 billion dollars, according to the FBI.

Here is the link: <https://www.ic3.gov/media/2019/190910.aspx>

"BEC attackers target senior-level employees rather than consumers, as it's easier to scam them out of large amounts. In one incident, we observed the scammers asking the target to transfer over US\$370,000. By requesting large amounts of money, the scammers only need to be successful a couple of times to make a profit," Symantec researchers explained.

There is a clear pattern you need to watch out for. It often begins with the scammers phishing an executive (using a whaling attack), dropping a Trojan, and gaining 24/7 access to that individual's email inbox. They research the organization and monitor the email account for as long as needed until the right circumstances arrive, then they pounce. They spoof the CEO's address and send messages to other individuals which are involved with the financial operations from a look-alike domain name that is one or two letters off from the target company's true domain name.

## Chapter 6

### Targeted Scams: Spear Phishing, Whaling, and More

\*\*\*

Cybercriminals understand that businesses are prime targets for attack. They use various methods such as whaling, spear phishing and social engineering to penetrate through the defenses of a company at the weakest links: people. CEO's and senior leadership are not immune to these scams – in fact, they are thoroughly researched by hackers looking for vulnerabilities.



# Chapter 7

## Understanding Cybercrime Losses and Exposures

No matter where you turn for statistics on cybercrime, the numbers are big—and they keep getting bigger. As you read this chapter, remember that more than 4.5 billion people now use the internet. Given a population this big, anything you measure is bound to be large, including cybercrime.

However, reporting and measuring losses is a tricky business. It's wise to treat such information with caution because crimes of all kinds tend to be underreported. Thus, it pays to remember that no matter how bad things look, they could be worse. Exercising due caution to minimize risk and exposure cannot be overhyped.

### *Cybercrime Reporting and Analysis*

In his seminal book [\*The Natural Mind\*](#), physician Andrew Weill suggests that philosophy and worldview exert incredible power over the ways humans perceive and interact with reality. He calls this viewpoint “What’s in it for me?” It reflects the perspective of someone who’s trying to make a case for some argument, or who wants to analyze a body of evidence to arrive at a set of “reasonable” conclusions.

Dr. Weill presents the idea that it’s always wise to consider what axe a report or an analysis is seeking to grind. This perspective can be as important as the facts or information someone presents while reasoning through to some sort of conclusion or call to action. Perhaps restating Dr. Weill’s maxim as “What’s in it for them?” is more to the point.

Many cybercrime reports come from organizations that are in the business of reacting to and countering cybercrime. Remember that for an organization that neutralizes cybercrime threats or apprehends and convicts cybercriminals, presenting a bleak picture of the cybercrime situation can be very good for business (or funding, as the case may be).

### *Trends in Cybercrime*

The FBI works in tandem with the National White-Collar Crime Center (NW3C) to operate the Internet Crime Complaint Center (IC3). Its website ([www.ic3.gov](http://www.ic3.gov)) is a clearinghouse for all kinds

## Chapter 7

### Understanding Cybercrime

#### Losses and Exposures

of information on internet crime. The site publishes regular scam alerts as new cybercrimes are discovered and documented. The IC3 also publishes annual reports on cybercrime trends and activities. As we write this book, the most recent version of that report, *2019 Internet Crime Report*, is available at [www.ic3.gov/media/annualreport/2019\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2019_IC3Report.pdf). Let's examine some choice selections to understand the size of cybercrime losses, the volume of cybercrime activities, and references to cybercrime in online media.

### ***Internet Crime Statistics***

Figure 26 shows the complaints and losses reported from 2015 through 2019.



***Figure 26 Annual number of complaints and losses received by the IC3, 2015 to 2019***

The reports to IC3 in 2019 alone totaled over \$3.5 billion in losses, averaging about \$6,419 per complaint. According to the FBI, businesses are attacked by ransomware alone over 4,000 times a day [23]. According to Varonis, hackers attack every 39 seconds, 48% of malicious email attachments are Microsoft Office files, and 94% of malware was delivered by email [24]. Their report also states that 43% of breaches involved small businesses and the average cost of a

ransomware attack on businesses is \$133,000. Cybriant, in a report about the global cost of cybercrime [25], estimates that 0.8% of global GDP is being lost to cybercrime.

## Losses Due to Cybertheft

Figure 26 also shows losses as reported in the *IC3 2019 Internet Crime Report*. The graph shows a steady progression of losses from the past to the near-present. Losses grew from \$1.1 billion in 2015 to \$3.5 billion in 2019, an increase of over 300% in just a few years. It's important to understand that the losses in IC3 are probably drastically understated because many people and businesses do not want the FBI to be involved. The IC3 figures are just what has been voluntarily reported to the FBI.

## How Cybercrime Gets Monetized

Most of the cybercrimes that produce actual cash or digital money are ransomware, ATM skimmers, and those that raid bank or brokerage accounts or obtain cash advances from credit cards (usually limited to 20% or so of a card's credit ceiling). All other cybercrimes require selling goods or information to produce cash. Not surprisingly, there's a thriving illicit economy where cybercriminals can trade ill-gained information or criminal services for cash. While reports on such exchanges represent only small and infrequent snapshots of this economy, they are interesting and show a thriving trading market at work.

Think back to the origin of phishing at AOL in the mid-1990s. Cybercrooks quickly began to trade "phish" for other things of value once the scam got going. Items traded included information about AOL accounts that could be used to impersonate a real account holder, steal his or her services, and make small purchases on somebody else's tab. Today's cybercrime market uses a combination of cash and barter, and it is basically an extension of the original "phish market," with many more items changing hands and a lot more cash involved. Table 4 lists some common items and describes the range of prices they can fetch on the cybercrime black market, according to Experian [26] and Symantec [27].

**Table 4 Going Rates for Stolen Cyber Info**

Item	Experian	Symantec
Social Security Number	\$1	\$0.10-\$1.50 (with DOB)
Online Payment Login	\$20-\$200	N/A
Driver's License	\$20	\$25-\$5000 (fake ID)

## Chapter 7

### Understanding Cybercrime

#### Losses and Exposures

Credit or debit card	\$5-\$110	\$1-\$45
Loyalty accounts	\$20	\$15-40% of value
Diplomas	\$100-\$400	N/A
Passports	\$1000-\$2000	\$25-\$5000 (fake ID)
Medical records	\$1-\$1000	\$0.10-\$35
Non-Financial Logins	\$1	N/A
Web admin credentials	\$2–60	N/A
Online banking account	N/A	0.5%-10% of value
Hacked email account (2,500)	N/A	\$1-\$15

The media is rife with stories about various kinds of web-based exchanges in such goods. You can look online and find reports on exchanges for stolen bank accounts and hijacked credit cards, for example. There's no question that a real underground economy is at work. In this economy, criminals with different skill sets are trading with each other to put together complete criminal operations, based on what they know and what others can contribute to their efforts.

## *A Terrible Spot for SMEs*

Larger enterprises typically pony up the cash to purchase cyber liability policies, or fraud insurance, so they obtain protection by spending money to hedge the risk. SMEs, on the other hand, normally don't purchase cybersecurity protection. This makes them "self-insuring," in the language of the insurance industry—a rather polite way of saying that they must eat any cyber fraud losses they incur. This is a tough situation. SMEs need to be aware of their exposure to fraud and perhaps to revisit their risk assessments. Who knows? Cybersecurity insurance may not be such a bad idea – if you can afford it!

To make this situation worse, SMEs apparently can't rely on their banks to implement complete or reasonable protection against **funds transfer fraud**, either. Many SMEs have brought lawsuits against banks, based on losses they incurred from fraudulent funds transfers. By and large, these suits charge that the banks involved violated section 4A-202 of the Uniform Commercial Code because they failed to provide "reasonable security" for that process.

*Section 4A-202 of the Uniform Commercial Code deals with how banks issue and accept payment orders, including online funds transfers.*

## ***The Patco Example***

A review of a summary of the allegations in the case between Maine-based construction company Patco and Ocean Bank is revealing. In *Patco Construction Company, Inc. versus People's United Bank d/b/a Ocean Bank*, Patco seeks to find its bank responsible for fraudulent funds transfers because the bank permitted multiple, larger-than-normal transfers to go through to offshore parties to which the firm had never transferred funds before. The allegations are also incredibly scary for what they say about the state of bank security and fraud protection for commercial customers:

- ✓ The bank failed to offer or use security tokens or one-time keys to authenticate identity for online transfers.
- ✓ The bank used an unreasonably low trigger value to send challenge-response queries to users so that all transactions required challenge-response, and attackers were able to harvest all that data.
- ✓ The bank did not check the originating Internet Protocol (IP) address for transaction requests, nor did it block requests that originated from addresses not already approved.
- ✓ The bank did not detect transfer fraud, even though transfer amounts were larger than any prior transfers, went to accounts that had never before been used, originated from IP addresses outside the customer's networks, and occurred on days when Patco normally did not make funds transfers.
- ✓ The bank offered no dual control option that would require two individuals to log in to complete payment transactions.
- ✓ The bank established a transfer limit that exceeded Patco's needs and allowed larger fraudulent transfers to go through.
- ✓ The bank failed to check Automated Clearing House (ACH) payment batches before submitting them for payment.
- ✓ The bank failed to send email alerts to Patco to alert them about unusual funds transfer requests.

This list is paraphrased from an article from the Information Law Group titled "Online Banking and 'Reasonable Security' Under the Law: Breaking New Ground?"

In 2011, the courts held that Ocean Bank was not at fault for the cyberheist, and in 2012, the U.S. Court of Appeals reversed that decision. The appeals court called the bank's security system "commercially unreasonable". [28]

## Chapter 7

### Understanding Cybercrime

#### Losses and Exposures

The following are desirable features when selecting a bank with which to conduct online funds transfers:

- **Multi-factor authentication:** Insists that the bank offer multi-factor authentication to authorize funds transfers online. (Chapter 18 covers multi-factor authentication in detail.) If the bank won't purchase and distribute security tokens such as RSA SecurID or some equivalent, ask it to institute a practice of sending a onetime authorization key.
- **Regular frequent review of all transfers:** Insist that the bank reviews your normal funds transfer activity. Set any challenge question trigger value high enough to skip small routine transfers but catch those that exceed a threshold value you select in concert with the bank.
- **Confirmation procedures for large transfers:** Insist that the bank instigate confirmation procedures for funds transfers over some specified amount. In the Patco case, the initial fraudulent transfer was \$20,000 higher than any single transfer made before. All subsequent fraudulent transfers were even larger than that!
- **Confirmation for unusual transfers:** Ask the bank to provide encrypted email or SMS confirmations for any unusual transfers that occur. Unusual might be defined as occurring on unusual days, for unusual amounts, and to new payees. The bank should hold all such transfers until approval is granted.
- **Acceptance of requests from only specified IP addresses:** Your organization can use IP blocking technology to register an IP address from which funds transfers may be ordered. The bank should then reject or require explicit telephone confirmation and approval for any alternate addresses from the account holder.
- **Isolate the computer.** Isolate the computer that has the capability to transfer funds from the network either physically or logically (using firewalls, IPSec, VLANs, etc.) so that it is far less likely to be pwned and then used to commit fraudulent transfers.

If any two of these stipulations had been met at the banks involved in lawsuits related to transfer fraud losses, then it's likely that none of those transfer requests would have succeeded. If banks won't police themselves, customers must force them to implement proper technical and procedural security measures. In the meantime, SMEs are on the hook for losses that might be incurred due to fraudulent funds transfers.

## *Reducing Phishing Risks*

In a successful business-related phishing attack, a cybercrook may gain access to an organization's bank accounts. In this case, all funds on deposit are at risk. But this also means

that a criminal can start changing account settings and security protocols. Such actions can facilitate transfer of funds offshore and delay fraud detection by the victim.

What does this mean? It means that, at a minimum, SMEs must contact their banks to understand current bank policies and procedures regarding account changes and online funds transfers. The best outcome of such a conversation would be to learn that no account policy changes can be implemented except under special circumstances. This might mean in person at a branch or in writing on company letterhead bearing the signature of a known and authorized company officer or representative. Such caution is not common; however, customers should set up such agreements with their banks as soon as possible.

SMEs and other organizations also need to manage risks associated with possible financial losses resulting from fraudulent funds transfers. At a minimum, this means reviewing their banks' online funds transfer security practices and procedures. Organizations should also review their banks' fraud detection and notification capabilities. Then account holders must decide how to implement their own safeguards to further secure funds transfers online. One way to stop most fraudulent transfers is to require the bank to initiate a phone call to a designated contact person before allowing any unusual or new online funds transfers.

In addition, the following steps can help you secure online bank transfers to reduce the possibility that a malware-based phishing attack could succeed:

1. **Set up a separate user account on any machines where funds transfers are made.** This account should then be used only for such transfers. Better yet, designate a specific machine to be used only for such transfers and for no other purpose.
2. **Don't share credentials between websites or services.** When logon credentials are shared between different websites or services the compromise of one can lead to a compromise of the other more quickly. Better yet, use MFA.
3. **Install antimalware software** (antivirus, antispymware, firewall, antirootkit, and so forth) on any machine used for funds transfers.
4. **Establish a regular schedule for funds transfers** (such as Tuesdays and Thursdays at 1 p.m.) and require prior confirmation with the bank via phone call or email to describe each transfer day's planned amounts and recipients. Don't allow any new or unusual funds transfer without a verified legitimate call or email that day.
5. **Establish a list of regular recipients for funds transfers.** Also establish maximum amounts allowed for each recipient. Financial staff and the bank should then carefully use these lists. All parties should question any off-list transfers or out-of-bounds amounts. The bank must get additional approvals (for example, from the finance department head, VP of finance, CFO, and so forth) before allowing such transfers to go through.

## Chapter 7

### Understanding Cybercrime

#### Losses and Exposures

6. **Finally, it's probably a good idea to meet with an insurance agent** to discuss your online funds transfer activity and to learn more about the costs and benefits of cybersecurity insurance. Cyber liability policies may not cost as much as you think. It's better to reject an option knowing its cost than never to ask.

## *Trends and Changes That Could Alter the Cybercrime Landscape*

The U.S. Court of Appeals decided that the bank's security measures were NOT commercially reasonable in the *Patco Construction Company, Inc. versus People's United Bank d/b/a Bank* case [29]. These and other cases like it have had a profound impact on cybercrime. Given that SMEs—such as small businesses, school districts, tax offices, police, and fire departments, and so forth—have been effective targets for fraudulent funds transfers, something must be done to stop these losses. Regardless of the court's decision, SMEs must take appropriate steps to ensure their security is adequate.

It's certain that the outcomes of legal cases will more clearly define the notion of “reasonable security” for online funds transfers. The definition that emerges from the legal process may require security measures such as those listed earlier in this chapter. Implementing such measures should drastically cut down on fraudulent funds transfers.

\*\*\*

Financial prudence and a general desire to limit or avoid such losses will force banks to change their online funds transfer practices and procedures no matter what happens in these cases. But as long as organizations are responsible for protecting (and insuring) themselves against losses due to fraud, they, too, should take more steps to protect and secure their funds transfers against fraud.



# Chapter 8

## Scary Reports and Statistics on Cybercrime

Surveys are a primary source of cybercrime analysis. Companies such as Gartner publish reports on cybercrime statistics through surveys completed by consumers and organizations. In some cases, survey participants volunteer data through complaint forms, while in others, individuals take more traditional fill-out-the-form surveys. Sample groups and sizes vary among surveys, as do selection criteria and analysis methods. The result is a complex mass of information from which to draw conclusions.

*Gartner is a leading technology research firm and prominent publisher of cybercrime analyses. Gartner employs professional survey companies to conduct technical research into hot topics affecting the global community. As part of Gartner's analysis process, survey companies ensure accurate and credible results by filtering out refusal rates and self-selection and by calculating tolerable margins of error.*

Cybercrime statistics serve many valuable purposes. One of the most important purposes is that they illustrate trends that drive responses and action. Cybercrime surveys are useful tools for identifying these trends and corresponding financial losses.

In this chapter, you'll learn that fraud encompasses all sorts of crime committed online and offline. You already know that fraudsters use computers and mobile phones to attract victims, target individuals and groups, and successfully hook many who should know better. Loss reports detail the financial and statistical impact of fraud as reported by survey participants. Unfortunately, the picture isn't complete because a majority of those losses are never reported.

Before we dive into loss statistics for recent years, let's take a look at some general cybercrime numbers for 2019 (from the 2020 Data Breach Investigations Report [30]):

- ✓ 70% of breaches were caused by outsiders
- ✓ 27% of malware incidents can be attributed to ransomware
- ✓ Organized criminal groups were behind 55% of breaches
- ✓ 46% of organizations got almost all their malware via email
- ✓ 72% of breaches involved large business victims
- ✓ 28% of breaches involved small business victims
- ✓ 22% of breaches involved phishing

## Chapter 8

### Scary Reports and Statistics on Cybercrime

Despite these sobering statistics, many SMEs believe the cost of fraud prevention isn't justified by the threats and potential losses. After all, criminals attack only big companies, right? Wrong. Although some criminals target specific individuals and groups, many cyberthieves cast wide nets and grab what they can. Depending on the scam, an SME is more likely to become a victim than a Fortune 500 company. It's in the numbers!

*A recent study by Chubb found that most SMEs (60% in Australia, 56% in Singapore, and 52% in Hong Kong) believe they are less of a target to cybercriminals than large organizations. [31]*

## Loss Reporting Trends and Information

The importance of cybercrime statistics can't be overstated. While there are compromises to collecting and analyzing cybercrime, the results of surveys have far-reaching implications. Crime statistics aren't simply an academic exercise; they also drive public, corporate, and security policies. Best practices are often built around these numbers. Studies provide the benchmarks by which online crime is measured and defense budgets are weighed.

While you can't always compare study for study, you can draw reasonable conclusions from the results, especially when confirmed across multiple unrelated studies. Instead of focusing on dollars, you can compare cybercrime by percentages. Of all the participants in a survey, how many were victims of fraud? What are the top-ranking forms of fraud? Which types of fraud are increasing year over year? What are the emergent threats?

### ***Statistics Don't Always Compare Apples to Apples***

*Always check the credibility of a source. That advice applies as much to online scams as it does to cybercrime statistics, which can be tricky for various reasons. Statistics may appear to tell a story, but they rarely reveal a complete picture, and despite the best intentions, they can be difficult to get right. Even when reliable studies from reputable sources are used, doubt may linger. Different companies often use different methods to analyze, classify, and calculate statistics, which makes it difficult to compare results directly.*

*Cybercrime statistics are especially challenging to analyze due to varying survey methods, different sample groups, and unreported losses. To make matters worse, consumers report crime only some of the time, and many institutions never file public reports. Financial institutions do report crimes to the Federal Deposit Insurance Corporation (FDIC) for analysis, but those details are never made public. The FDIC reports only performance statistics publicly; it doesn't disclose details of crimes.*

*Research methods also vary from study to study. Each survey involves specific selection criteria, uses idiosyncratic screening methods, and involves varying margins of error.*

*Every study covers some specific time frame and sample group, but these time frames and groups seldom overlap or converge. Many classify and categorize the same crimes differently. The global nature of online fraud also makes investigation, prosecution, and analysis challenging. The upshot of all this is captured nicely in the title for this sidebar and is worth remembering as you read and digest cybercrime statistics in this book and elsewhere.*

## The Many Forms of Modern Fraud

Financial scams are vast and varied. Most studies focus on email scams, identity theft, and credit fraud—but these crimes hardly capture the full spectrum of possibilities. Scams constantly evolve to adapt to modern themes, such as the rise of “hitman scams” from would-be assassins to extort money from victims. (In a hitman scam, an alleged assassin extorts money through the threat of murder for hire.) The internet provides a wealth of opportunity for fraudsters. It also provides access to millions of potential victims on which to practice endless variations on old scams. Tracking trends helps determine where criminals are focusing their attention and which groups are most susceptible.

Economic, healthcare, and online job scams all represent modern twists on old cons. Yet these are only a few of the emerging and explosive trends in internet financial fraud. Playing on common fears, fraudsters have used economic crisis, healthcare laws, long-term unemployment, and trustworthy brands to defraud victims of billions over the past decade. Scams also adapt to new media, such as social networks, text messages, and VoIP technology.

*The Internet Crime Complaint Center (IC3) publishes studies based on victim complaints that span the spectrum of cybercrime. However, even the IC3 admits that its statistics are imperfect. Complaints are heavily influenced by consumer perception, which is often itself flawed, so two victims of the same crime might report it differently.*

Conventional fraud is a vast and complex subject that’s fraught with many challenges. The greatest problem related to categorizing and analyzing fraud comes from the number of variations on each scam. Consumers and organizations broadly define fraud as it overlaps schemes and technologies, such as smishing, for identity theft to commit financial fraud. Confidence in trend analysis requires clean data from credible sources, and representative samples are only part of that picture.

Financial fraud doesn’t occur in a vacuum. Malware infections often precede fraud. A very common example involves the sale of fake antivirus software. But the product is only bait; the hook was bogus support from a live agent. This type of fraud is known under various names, including the PC Support Scam and the Windows Support Scam.

## Chapter 8

### Scary Reports and Statistics on Cybercrime

Fraud against financial institutions often implies accessory crimes or other criminal activity. A system intrusion may lead to account takeovers, which results in stolen funds. Smishing for identity theft often leads to credit fraud, and phishing is the primary source for advance-fee fraud. One crime often begets another, forming a chain of criminal events, one after the other.



#### **Advance-Fee Fraud**

An **advance-fee fraud** is a type of scam in which a cybercriminal persuades a potential victim to help transfer a substantial amount of money to an account. The victim is offered a commission for facilitating the transaction or multiple transactions. The Nigerian scam, also called the **419 scam**, is a prime example of advance-fee fraud.

## *The Iceberg of Unreported Losses*

Beneath the surface of known cybercrime statistics hides a larger body of unknown data. Unreported losses are a major unknown quantity in assessing financial damages, and they are the reason such statistics are seen by some as unreliable. Most industries and many companies don't reveal the costs of fraud openly or freely, so those numbers come mostly from consumer surveys. Schools and colleges also refrain from reporting certain crimes due to social stigmas or concerns about their reputations.

Organizations conceal the dangers of doing business online, such as intrusions and theft, because knowledge of such problems drives off good business. Personal and financial data theft lowers customer confidence. It gives the impression of vulnerability, which decreases consumer trust in a company. Fraud victims also hesitate to report cybercrimes for a variety of reasons, such as embarrassment, privacy, and mistrust. Because few companies and consumers report cybercrimes, all but the tip of the iceberg remains unseen.

### ***The Dark Figure of Crime***

*Criminologists and sociologists have a term for unreported losses and undiscovered crime: the **dark figure of crime**. It's the amount of crime that remains undiscovered and unknown. That gap in knowledge always casts doubt on the reliability of official crime statistics. As bad as reports may seem, the reality is likely to be far worse!*

Unreported crime is troublesome for statistics because it casts a shadow of doubt. Several organizations conduct independent surveys to capture some of those unreported crimes, but many remain unknown and uncounted. Sometimes law enforcement agencies conduct their own crime surveys. In every case, refusal rates (that is, nonparticipants) are high, but such studies manage to uncover previously unreported crimes.

## Loss Reports: 2016–2019

The IC3 claims there is growing public interest in the average monetary loss due to internet fraud. The IC3 therefore provides loss estimates across the general population by crime and expresses this information in mean and median averages. Mean averages are sensitive to extreme high and low losses. Median averages represent the midpoint and are less susceptible to extremes.

### Reported Losses for 2019

In 2019, the IC3 received 467,361 complaints and referred many of them to law enforcement for a total of \$3.5 billion in damages. And that’s just for the victims who spoke up. Countless others lost additional unknown sums.

Among the most prominent scams of 2019 by the IC3’s estimate was Extortion, with 43,101 complaints. Confidence/Romance fraud accounted for 19,473 of referred complaints, followed by Identity Theft fraud at 16,043 and Harassment at 15,502. Figure 27 and Figure 28 list the top IC3 complaint categories for 2019.

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	114,702	Lottery/Sweepstakes/Inheritance	7,767
Non-Payment/Non-Delivery	61,832	Misrepresentation	5,975
Extortion	43,101	Investment	3,999
Personal Data Breach	38,218	IPR/Copyright and Counterfeit	3,892
Spoofing	25,789	Malware/Scareware/Virus	2,373
BEC/EAC	23,775	Ransomware	2,047
Confidence Fraud/Romance	19,473	Corporate Data Breach	1,795
Identity Theft	16,053	Denial of Service/TDoS	1,353
Harassment/Threats of Violence	15,502	Crimes Against Children	1,312
Overpayment	15,395	Re-shipping	929
Advanced Fee	14,607	Civil Matter	908
Employment	14,493	Health Care Related	657
Credit Card Fraud	14,378	Charity	407
Government Impersonation	13,873	Gambling	262
Tech Support	13,633	Terrorism	61
Real Estate/Rental	11,677	Hacktivist	39
Other	10,842		

*Figure 27 Fraud by Victim Count for 2019*

## Chapter 8

### Scary Reports and Statistics on Cybercrime

Source: [https://pdf.ic3.gov/2019\\_IC3Report.pdf](https://pdf.ic3.gov/2019_IC3Report.pdf)

By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$1,776,549,688	Employment	\$42,618,705
Confidence Fraud/Romance	\$475,014,032	Civil Matter	\$20,242,867
Spoofing	\$300,478,433	Harassment/Threats of Violence	\$19,866,654
Investment	\$222,186,195	Misrepresentation	\$12,371,573
Real Estate/Rental	\$221,365,911	IPR/Copyright and Counterfeit	\$10,293,307
Non-Payment/Non-Delivery	\$196,563,497	Ransomware	**\$8,965,847
Identity Theft	\$160,305,789	Denial of Service/TDoS	\$7,598,198
Government Impersonation	\$124,292,606	Charity	\$2,214,383
Personal Data Breach	\$120,102,501	Malware/Scareware/Virus	\$2,009,119
Credit Card Fraud	\$111,491,163	Re-shipping	\$1,772,692
Extortion	\$107,498,956	Gambling	\$1,458,118
Advanced Fee	\$100,602,297	Health Care Related	\$1,128,838
Other	\$66,223,160	Crimes Against Children	\$975,311
Phishing/Vishing/Smishing/Pharming	\$57,836,379	Hackivist	\$129,000
Overpayment	\$55,820,212	Terrorism	\$49,589
Tech Support	\$54,041,053		
Corporate Data Breach	\$53,398,278		
Lottery/Sweepstakes/Inheritance	\$48,642,332		

**Figure 28 Fraud by Victim Loss for 2019**

Source: [https://pdf.ic3.gov/2019\\_IC3Report.pdf](https://pdf.ic3.gov/2019_IC3Report.pdf)

## Reported Losses for 2018

In 2018, the IC3 received 351,937 complaints and referred many of them to law enforcement for a total of \$2.7 billion in damages.

Among the most prominent scams of 2018 by the IC3's estimate was Extortion, with 51,146 complaints. Personal Data Breaches accounted for 50,642 of referred complaints, followed by Phishing/Vishing/Smishing/Pharming at 26,379 and BEC/EAC at 20,373. Figure 29 and Figure 30 list the top IC3 complaint categories for 2018.

## 2018 CRIME TYPES

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Non-Payment/Non-Delivery	65,116	Other	10,826
Extortion	51,146	Lottery/Sweepstakes	7,146
Personal Data Breach	50,642	Misrepresentation	5,959
No Lead Value	36,936	Investment	3,693
Phishing/Vishing/Smishing/Pharming	26,379	Malware/Scareware/Virus	2,811
BEC/EAC	20,373	Corporate Data Breach	2,480
Confidence Fraud/Romance	18,493	IPR/Copyright and Counterfeit	2,249
Harassment/Threats of Violence	18,415	Denial of Service/TDoS	1,799
Advanced Fee	16,362	Ransomware	1,493
Identity Theft	16,128	Crimes Against Children	1,394
Spoofing	15,569	Re-shipping	907
Overpayment	15,512	Civil Matter	768
Credit Card Fraud	15,210	Charity	493
Employment	14,979	Health Care Related	337
Tech Support	14,408	Gambling	181
Real Estate/Rental	11,300	Terrorism	120
Government Impersonation	10,978	Hacktivist	77

*Figure 29 Fraud by Victim Count for 2018*

## Chapter 8

### Scary Reports and Statistics on Cybercrime

Source: [https://pdf.ic3.gov/2018\\_IC3Report.pdf](https://pdf.ic3.gov/2018_IC3Report.pdf)

By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$1,297,803,489	Tech Support	\$38,697,026
Confidence Fraud/Romance	\$362,500,761	Harassment/Threats of Violence	\$21,903,829
Investment	\$252,955,320	Misrepresentation	\$20,000,713
Non-Payment/Non-Delivery	\$183,826,809	IPR/Copyright and Counterfeit	\$15,802,011
Real Estate/Rental	\$149,458,114	Civil Matter	\$15,172,692
Personal Data Breach	\$148,892,403	Malware/Scareware/Virus	\$7,411,651
Corporate Data Breach	\$117,711,989	Health Care Related	\$4,474,792
Identity Theft	\$100,429,691	Ransomware	*\$3,621,857
Advanced Fee	\$92,271,682	Denial of Service/TDoS	\$2,052,340
Credit Card Fraud	\$88,991,436	Re-Shipping	\$1,684,179
Extortion	\$83,357,901	Charity	\$1,006,379
Spoofing	\$70,000,248	Gambling	\$926,953
Government Impersonation	\$64,211,765	Crimes Against Children	\$265,996
Other	\$63,126,929	Hacktivist	\$77,612
Lottery/Sweepstakes	\$60,214,814	Terrorism	\$10,193
Overpayment	\$53,225,507	No Lead Value	\$0.00
Phishing/Vishing/Smishing/Pharming	\$48,241,748		
Employment	\$45,487,120		

**Figure 30 Fraud by Victim Loss for 2018**

Source: [https://pdf.ic3.gov/2018\\_IC3Report.pdf](https://pdf.ic3.gov/2018_IC3Report.pdf)

## Reported Losses for 2017

In 2017, the IC3 received 284,000 complaints and referred many of them to law enforcement for a total of \$1.42 billion in damages. And that's just for the victims who spoke up. Countless others lost additional unknown sums.

Among the most prominent scams of 2017 by the IC3's estimate was Non-Payment/Non-Delivery, with 84,079 complaints. Personal Data Breaches accounted for 30,903 of referred complaints, followed by Phishing/Vishing/Smishing/Pharming at 25,344 and Overpayment at 15,502. Figure 31 and Figure 32 list the top IC3 complaint categories for 2017.



By Victim Count			
Crime Type	Victims	Crime Type	Victims
Non-Payment/Non-Delivery	84,079	Misrepresentation	5,437
Personal Data Breach	30,904	Corporate Data Breach	3,785
Phishing/Vishing/Smishing/Pharming	25,344	Investment	3,089
Overpayment	23,135	Malware/Scareware/Virus	3,089
No Lead Value	20,241	Lottery/Sweepstakes	3,012
Identity Theft	17,636	IPR/Copyright and Counterfeit	2,644
Advanced Fee	16,368	Ransomware	1,783
Harassment/Threats of Violence	16,194	Crimes Against Children	1,300
Employment	15,784	Denial of Service/TDoS	1,201
BEC/EAC	15,690	Civil Matter	1,057
Confidence Fraud/Romance	15,372	Re-shipping	1,025
Credit Card Fraud	15,220	Charity	436
Extortion	14,938	Health Care Related	406
Other	14,023	Gambling	203
Tech Support	10,949	Terrorism	177
Real Estate/Rental	9,645	Hacktivist	158
Government Impersonation	9,149		

*Figure 31 Fraud by Victim Count for 2017*

## Chapter 8

### Scary Reports and Statistics on Cybercrime

Source: [https://pdf.ic3.gov/2017\\_IC3Report.pdf](https://pdf.ic3.gov/2017_IC3Report.pdf)

By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$676,151,185	Misrepresentation	\$14,580,907
Confidence Fraud/Romance	\$211,382,989	Harassment/Threats of Violence	\$12,569,185
Non-Payment/Non-Delivery	\$141,110,441	Government Impersonation	\$12,467,380
Investment	\$96,844,144	Civil Matter	\$5,766,550
Personal Data Breach	\$77,134,865	IPR/Copyright and Counterfeit	\$5,536,912
Identity Theft	\$66,815,298	Malware/Scareware/Virus	\$5,003,434
Corporate Data Breach	\$60,942,306	Ransomware	\$2,344,365
Advanced Fee	\$57,861,324	Denial of Service/TDoS	\$1,466,195
Credit Card Fraud	\$57,207,248	Charity	\$1,405,460
Real Estate/Rental	\$56,231,333	Health Care Related	\$925,849
Overpayment	\$53,450,830	Re-Shipping	\$809,746
Employment	\$38,883,616	Gambling	\$598,853
Phishing/Vishing/Smishing/Pharming	\$29,703,421	Crimes Against Children	\$46,411
Other	\$23,853,704	Hacktivist	\$20,147
Lottery/Sweepstakes	\$16,835,001	Terrorism	\$18,926
Extortion	\$15,302,792	No Lead Value	\$0
Tech Support	\$14,810,080		

**Figure 32 Fraud by Victim Loss for 2017**

Source: [https://pdf.ic3.gov/2017\\_IC3Report.pdf](https://pdf.ic3.gov/2017_IC3Report.pdf)

## Loss Projections

Online fraudsters are expected to become even more ambitious in the future. Criminals are taking bolder risks to combat the rising tide of technology and training against online fraud. **Security awareness training** is crucial to defeat online fraud, as technology cannot protect against careless or foolish behavior.

## ***Emerging Trends***

Fraud trends show signs of moving away from “net” phishing and toward spear phishing. Instead of general attacks against broad audiences, criminals are increasingly targeting specific groups and individuals. We can certainly expect more of the same: As phishing proves less viable, scammers will turn to ransomware, smishing, and vishing and other new variants. Link manipulation, fake trial offers, advance-fee loans, and job scams will continue to thrive.

Mobile threats rose by 50% between 2017 and 2018 [32] according to researchers at *Check Point*. Like computers, popular mobile platforms attract malware. And why shouldn't they? Mobile phones are computers and are subject to the many of the same sorts of attacks. The connectivity options are astounding: infrared, Bluetooth, and texting provide some of the many possible inroads.

General consumers aren't the only targets. Online merchants are victims, too. A common scam targeted online sellers through fake receipts generated by a malicious program. In another case, a malicious holiday greeting pretending to be from the White House specifically targeted government workers. The Federal Trade Commission (FTC) issued an alert in April 2020 regarding scammers who sell facemasks to protect against COVID-19. The masks were never delivered. [33]

## ***Speculation Abounds***

Scam artists are constantly aware of the latest online trends. Successful cons leverage timing and circumstances to strike as opportunities arise. Speculative articles such as McAfee's *Cyber Threats* and the Better Business Bureau's *Top Ten Scams*, published annually, give glimpses into the possible future this foreshadows.

Uniform Resource Locator (URL) shortening services, where the original longer URL is converted to a shortcut URL which obfuscates potential maliciousness, are very popular with online scammers. Symantec states that 1 in 10 URLs were malicious in 2018. [27]

Fraud trends often follow behind malware trends. Emerging malware threats against mobile platforms can lead to attacks to steal information. Twitter is constantly a target for intrusions and scams alike, and privacy mishaps like those involving Facebook can put users at risk of fraud.

## ***Gaping Security Holes Pose Big Risks***

People are always the weakest link in any security chain. People make the poor decisions that undermine privacy and undercut security. An undereducated user is the greatest threat to any secure environment. One person's negligence can put an entire company at risk.

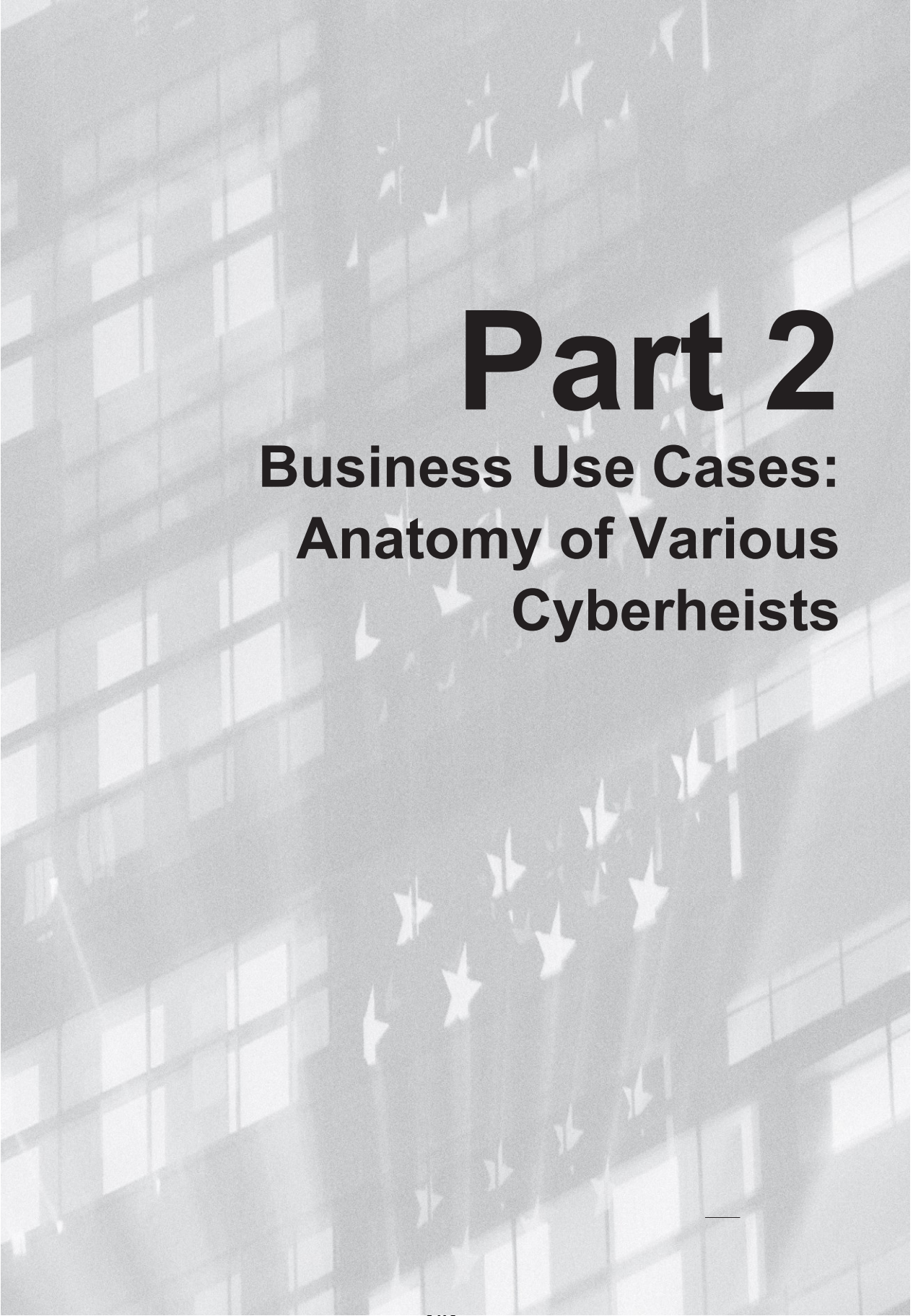
## Chapter 8

### Scary Reports and Statistics on Cybercrime

In Brazil, a senior bank official was persuaded by three Nigerian scammers to transfer a total of \$242 million from the bank, which brought about its collapse. It was a landmark Nigerian scam. A Nigerian commission eventually awarded \$17 million to the defunct bank's lawyer, and the scammers forfeited assets worth \$121.5 million. But the damage was done: The bank went bankrupt, and the customers went broke.

\*\*\*

As people become increasingly connected, they aren't becoming more security conscious. Popular applications with poor coding or weak security practices may enable criminals to overtake systems and accounts. Unrestricted applications on social networks may access private information and enable identity fraud. And "friendly fire" malware—the kind where grandma posts a rave review about the iPad she doesn't even own—will increase in frequency. Get ready!



# **Part 2**

## **Business Use Cases: Anatomy of Various Cyberheists**



# Chapter 9

## Bank Scams

In simple terms, a **bank scam** is an attempt by unscrupulous persons or organizations to acquire financial assets from individuals or organizations, including SMEs. The focus of this chapter is not on fraud committed against the banking industry. Rather, it is on bank fraud committed against SMEs, often through or by their employees.

Large corporations routinely purchase fraud insurance or cyber liability policies, but smaller organizations often do not. Although it's good protection, many SMEs see the insurance as an unnecessary expense; after all, the majority of SMEs believe cybercriminals target large corporations. However, SMEs are highly vulnerable targets. If a malicious attempt against a small business is successful and of large enough scope, the company might not be able to recover.

### *A Sampler of Banking Scams*

Many of the methods used to commit banking scams against SMEs have already been presented in this book. For example, social engineering techniques include phishing and smishing to acquire individual or corporate login access at an institution. An organization's employees or customers can also be exposed to fraud attempts via email, social networking sites, and Twitter. Criminals sometimes use malicious programs to drain an organization's assets, which can damage or ruin its reputation or business viability. They may target not only SMEs, but also federally sponsored enterprises.

### ***Attackers Target Credit Card Processing***

The credit card processing systems in Eastern Europe suffered from large numbers of attacks in early 2017. The criminals managed to get into the bank's infrastructure and after gaining access to the credit card processing systems, they increased overdraft limits on credit cards. Additionally, antifraud systems were disabled to prevent fraud warnings from being sent to the security people. They used people in other countries to create false identities and used those to create accounts in branches of the banks. After they had the accounts, they requested debit cards which they then used to withdraw money from ATM machines. [34]



## ***Hackers Use Malware to Steal from Taiwanese Bank***

Close to \$60 million was stolen from the Far Eastern International Bank in Taiwan in 2017. A pair of hackers used malware to steal money from the bank using fraudulent messages sent with the SWIFT interbank messaging network. SWIFT is used by banks and over 200 countries to transfer funds. After the fake transactions were detected, the bank was able to garner the help of banks and other countries and recovered most of the money. Three people were involved in committing the crime and two of them were taken into custody. [35]

## ***World's Biggest Cyber Robbery***

A group of Russian hackers spent two years hacking more than 100 financial institutions all over the world. When the plot was finally uncovered, they managed to steal more than £650 million. They hit banks in countries all over the world, including Japan, China, the U.S., and Europe. These hackers used computer viruses to infect computers, then installed malware that gathered information from each financial institution. This even included video feeds within the offices of these businesses.

They used this data to impersonate online staff and trick them into transferring money to dummy accounts, which they then withdrew from ATM machines. They sent commands to the ATM machines to program them to dispense money at specific times without an ATM card. The machines actually ejected so much money at those times that cameras show piles of money being swept up by anyone who happened to be passing during those times. A spokesman for Kaspersky Lab said: "The plot marks the beginning of a new stage in the evolution of cybercriminal activity, where malicious users steal money directly from banks, and avoid targeting end users." [36]

## ***JP Morgan Chase Hacked***

In late 2015, four men were charged with hacking into several financial institutions from 2012 to 2015, stealing the data of more than 100 million people, including over 80 million customer accounts at JP Morgan Chase. Three men were identified – Gery Shalon, Joshua Samuel Aaron, and Ziv Orenstein – and charged with 23 counts of fraud related crimes. The fourth was not identified.

They were able to gain access to six other financial businesses, news sites, online stockbrokers and software companies. Their victims included Dow Jones, Scottrade, and ETrade. They used numerous methods to hack into the computing resources of these companies, including social engineering to gain login information for ETrade and Scottrade.

One method they used to gain access was to take advantage of a vulnerability in the operating system. A patch had been available for over a year, yet was not applied. The hackers used the



names, addresses, and other contact information that they gained (no credit card numbers, passwords, or social security numbers were compromised) to operate a stock manipulation scheme, a dozen internet gambling sites, and a Bitcoin exchange. [37]

## **Account Information Scams**

As mentioned elsewhere in this book, cybercrooks use phishing, smishing, and vishing scams to steal information. These fraudsters are looking for information such as names, dates of birth, bank login credentials, social security numbers, and other identifying data. Cybercrooks can then use the information they obtain to access banking and business accounts for the individual and siphon off assets.

Cybercrooks also use these techniques to target employees or partners of SMEs in order to access an organization's assets. They might use these methods against an accountant or a bookkeeper, for example. If the responsible individual can be convinced to click a link or open an attachment, the fraudster wins. Keylogger and Trojan software partner up to help the criminal eventually steal bank account information and funds.

*The difference between phishing and the other methods just mentioned is the delivery system used. Email phishing scams are common. But due to the ubiquitous use of smartphones and texting, it's also easy to attempt fraud via handheld devices, using Voice over Internet Protocol systems. Another form of fraud is called **phreaking**, and it involves directly hacking telecommunications systems.*

## **Patco Construction Company, Inc. versus People's United Bank d/b/a Ocean Bank**

Cases of bank fraud can set a banking customer and its financial institution at odds. As described in Chapter 7, Patco Construction Company sued its bank, People's United Bank d/b/a Ocean Bank, for failure to "protect its customers' funds against theft."

Ocean Bank said that it employed extremely sophisticated "behind-the-scenes" security techniques to monitor its accounts and protect them from online attacks. However, the Patco lawsuit claimed that the bank's security measures were inadequate and allowed an attack that resulted in Patco funds being improperly transferred. The type and pattern of the transactions were atypical for Patco. In addition, funds were transferred to accounts with which Patco had never previously transferred funds. Further, according to the suit, Ocean Bank allowed the fraudsters to draw on a line of credit that Patco had with the bank in order to remove an additional US\$200,000 of funds beyond the original transfers.

## Consequences to Banks and Customers Alike

If a bank fails in its duty to properly protect a customer's funds, the customer may sue the bank to recover the lost funds. However, most cases are settled out of court. Patco versus People's United Bank was the first case involving fraudulent online corporate funds transfers that went to trial, and after appeal, the bank was determined to be at fault. The Experi-Metal Inc versus Comerica Bank case also found the bank was at fault for lack of proper security.

These cases should motivate banking institutions to conduct internal security reviews to protect their customers and the banks themselves. It's critical for banks of all sizes to verify that they're taking all reasonable measures to prevent fraud that could result in loss of customer funds.

### **Banking Fraud and Social Networking**

*Criminals can use social networking venues, such as Facebook and Twitter, the same way they use email and texting to perpetrate crimes against individuals and organizations. A cybercrook can spoof a Facebook or Twitter account, and then send a Facebook message or tweet to an SME employee on the weekend. The message might purport to be from a coworker, requesting that person's login information because the "coworker" forgot his or her own and needs it to finish an important project. If the SME employee takes the message at face value and doesn't use another means of verifying the sender's identity, he or she may end up transmitting the login information to a malicious person. That person then has access to whatever accounts, records, and assets the SME employee manages. If the employee has access to the company's bank accounts, the malicious person can drain large sums of money or other resources, and the soonest the crime will be discovered is the following Monday. The SME employee will be left holding the "smoking gun."*

## SMEs Vulnerable to Banking Scams

The 2019 State of Cybersecurity revealed some startling facts about how vulnerable SMEs are to banking scams: [38]

- ✓ 66% of SMBs experienced a cyber attack.
- ✓ An attack causes damages of \$1.2 million on average.
- ✓ Disruptions to normal operations cost US\$1.9 million on average.
- ✓ 46% of SMBs suffered from an attack involving the compromise of employee passwords.
- ✓ 53% said phishing and social engineering were their number one attack experience.

- ✓ 82% of SMBs reported that their antivirus did not stop malware.

As mentioned earlier in this chapter, many SMEs aren't covered under private fraud insurance. In addition to having their employees divulge sensitive data as a result of phishing and other social engineering scams, bank accounts for SMEs are vulnerable to the same sort of attacks as personal bank accounts.

## ***SMEs and Banking Trojans***

Malicious persons can take advantage of unpatched computer vulnerabilities. Newly developed malware is designed to go undetected by traditional antivirus solutions. Various malware types can gather sensitive data from SME computers and servers, including banking authentication information. A single SWIFT attack can remove hundreds of thousands of dollars from an SME's bank account in a short time. Because SMEs traditionally don't monitor their bank accounts daily, the theft might go undiscovered for days.

*The probability of recovering the stolen funds declines sharply more than 24 hours after the theft.*

Banks aren't obligated to reimburse victim SMEs for their losses. However, they do generally work with a company to attempt to reverse any fraudulent asset transfers. However, the window for doing so successfully is only about 24 hours. Corporate accounts are responsible for any Automated Clearing House debits after two days. If an SME fails to review its corporate bank accounts daily, it may not discover the fraudulent money transfers in time to avoid liability.

## ***SMEs and Federal Investigations***

Banking fraudsters target SMEs for a number of reasons. SMEs are vulnerable to viruses and other malware, and they tend not to oversee their bank accounts very closely. In addition, the FBI may not open an investigation of online bank fraud because their minimum loss thresholds range from US\$100,000 to US\$500,000 and a particular victim's damage may not meet the threshold. Many SMEs are unlikely to have accounts that contain more than, say, US\$200,000. So, while these amounts may fall below the level that triggers a federal investigation, they probably represent all the funds the organization has. For small businesses, such losses will effectively drive them into bankruptcy.

## ***Large-Scale ACH Fraud***

A single SME's loss may not draw the attention of federal authorities, but the combined losses of a large number of SMEs will. **ACH fraud** takes advantage of computer vulnerabilities and malware to transfer millions of dollars in bank funds out of numerous SME accounts. The fraudsters parcel

## Chapter 9

### Bank Scams

those funds out to **money mules**—people who are duped into thinking that they are managing payroll transfers for international companies. The mules receive money transfers of less than \$10,000 per transfer to avoid triggering a suspicious activity report (SAR) from the bank. Once the mule makes the required overseas wire transfer, those funds are usually gone forever.

*Amounts as low as \$5,000 can trigger a SAR. However, the mandatory requirement is for amounts is \$10,000 or more. Therefore, most ACH fraud transactions are around \$9,000.*

The ACH scamming mechanism is an example of spear phishing. You learned about spear phishing in Chapter 6 and will learn about ACH scams in depth in Chapter 12.

### **Payroll Fraud**

Sometimes, malicious parties can add themselves or their proxies to the payroll of an SME. When the bank issues biweekly electronic paychecks, the fraudsters are “paid” along with the real employees. Remarkably, individuals can be added to a company’s payroll at the SME’s bank of record without the required documentation (for example, a canceled check or deposit slip from the employee’s bank or a completed payroll authorization form). In this case, the bank, not the SME, has failed to take the proper protective measures. This type of fraud requires a coordinated effort, including soliciting the services of a large number of money mules. However, the rewards for the thieves are vast, and the money mules are expendable.

## *Understanding Scamming Mechanisms*

Many of the common methods criminals use to commit bank fraud against SMEs have been mentioned in earlier chapters and in this chapter. Phishing and similar scams are among these common methods. Malware attacks are fairly common occurrences for both individuals and organizations. However, the malware that fraudsters use against SMEs and their banking institutions often contains keyloggers. To get keyloggers on systems, scammers must induce individuals who have the authority to make online asset transfers (such as banking staff) to click a link in an email. Clicking the link subjects the user to a malware download. Such email is crafted to look like a legitimate business message, such as a notice to upgrade or patch the user’s computer email client or office suite.

Malicious people may exploit numerous vulnerabilities, including known computer vulnerabilities that haven’t been patched. Also, malware that has been developed recently or that is designed to evolve to evade signature-based antivirus and intrusion detection systems has become increasingly common.

*Some desktop and server computers in banking firms used by SMEs fail to use antivirus software at all. In addition, SMEs and banks sometimes either don't have firewalls installed or have firewalls that are poorly configured and don't provide adequate defense against attacks. Alas, this makes the work of fraudsters extra easy.*

In summary, fraudsters take advantage of poor SME oversight of bank accounts. This lax attention allows the crooks to transfer large sums out of bank accounts. Sometimes such thefts go unnoticed for as long as several days, allowing the fraudsters to transfer assets out of the country.

## How to Avoid Bank Scams

Often, employees—including managers and administrators—can be weak links in even an otherwise well-defended company's online security. The first step in preventing SME/bank fraud is to thoroughly train all personnel in the methods fraudsters can use against them to make fraudulent monetary transfers. This includes teaching employees about various social engineering scams, such as phishing.

### **Training Is Key**

Adequate training also means notifying employees that there are no safe communications conduits. Some managers might believe that employees are only vulnerable to phishing-type scams via email, and consider texting, phone, Twitter, and social networking sites to be more secure. That's not true—threats can be delivered via any communication channel and lurk on all kinds of websites. The best defense is being able to recognize them regardless of their source.

*If applications such as Twitter and websites such as Facebook aren't required for business purposes, an organization should consider using business policies and technical means to prevent their use in the workplace.*

After an organization trains staff to be aware of how they can be exploited, it should provide regular follow-up training. This training needs to be more than a few times a year and optimally would occur at least monthly. While people are usually vigilant immediately after they have been trained, their threat awareness tends to diminish over time. However, the threat of fraudulent thefts continues to grow, and new variations appear every day.

Often, SMEs, including regional banks, don't have the proper IT or security staff to provide such training. In these cases, the company's best option is to hire a third-party security or training vendor. It's also possible to train in-house staff to provide this service. However, the appropriate staff may eventually leave the company. Or they might not have time to keep their training and security skills current, which means they would fail to keep the rest of the staff apprised of the latest threats and appropriate countermeasures or avoidance techniques. Chapter 23 provides a

## Chapter 9

### Bank Scams

lot of information on security awareness training: tips for delivering it in-house, and third-party resources that provide current, on-demand, web-based training for a reasonable price.

### ***Technical Defenses Are Important, Too***

An organization may need to hire third-party security vendors to assess the organization's level of vulnerability and to suggest and implement improvements. They should recommend policy changes, technical controls, and training. The technical controls can include installing and configuring antivirus, firewall, and intrusion detection solutions to optimize the company's defense against scams.

*Both SMEs and the banks they use should utilize such resources to improve their security. SMEs should also investigate and choose to do business only with financial institutions that use the same precautions and that can ensure an ongoing commitment to online security.*

Employees are sometimes taken in by social engineering scams. Therefore, an organization should reduce employee computer privileges to the minimum required to perform their job functions. Not everyone in an organization needs to be able to operate with administrator rights on both the local computer and network levels. Also, the organization should remove any public access to the names and contact information for staff members responsible for asset transfers. This way, fraudsters will have more difficulty learning who to target.

Signature-based antivirus solutions have proven less effective against malware used for banking scams than methods of detection that don't depend on predefined digital "signatures" of previously known malware. Therefore, an organization should supplement these techniques with **application whitelisting**, allowing only known and previously approved software to execute within the company's computer system. The organization should also consider using heuristic detection or AI rather than or in addition to a signature-based antivirus solution on computers that may access online banking accounts.

***Heuristic detection*** is a method of malware detection that doesn't depend on knowing the specific signature characteristics of a known type of malware. Heuristic methods look for more generic elements and actions of programs that are indicative of viruses or other malware rather than those types of legitimate software that are expected to be found on computers.

\*\*\*

Businesses of all sizes are regularly attacked via social engineering and other scams. As a result, organizations must train users to be aware of their vulnerabilities and to take proper actions when a scam is suspected.

# Chapter 10

## Credit Card and Epayment Scams

Online merchant fraud is a multi-billion-dollar business. Any vendor offering physical or digital merchandise for sale online is a target. Numerous stand-alone fraud-detection device and software solutions are available, but none of them are perfect. In any case, many SMEs often believe they can't afford to purchase such protection. As with banking scams, SMEs are especially vulnerable to credit card or epayment fraud—but no online merchant is immune.

As with many other forms of fraud, credit card scams are not only perpetrated by individuals, but also by criminal organizations, usually from outside the United States and Canada. If a fraudster successfully purchases merchandise from an online vendor using a stolen credit card, the item often ships overseas before anyone detects the theft. If ecommerce fraud involved one laptop here and one flat-panel TV there, it wouldn't be much of an issue. But ecommerce fraud has a vast scope. Every organization—from “mom-and-pop” shops to *Fortune 500* companies—is at risk.

### *The World of Credit Card Scams*

Most people are aware of credit card scams that affect individual cardholders. We hand our cards over to restaurant waiters who disappear to a secluded register. They could easily copy the number (or scan it using a small card swipe hidden in their pocket, under the table or elsewhere) and use it to buy something online. We enter our card number (the first time, at least) when making a purchase at Amazon. A keylogger covertly installed on our computer could be transmitting the number to a malicious fraudster. We get a call from our bank, saying that there's been “unusual activity” on our credit card account and asking us to verify our card number. Have we been ripped off, or are we being scammed at that moment by the caller? Cybercriminals use stolen credit cards to purchase items from shopping and music sites. They also use stolen card numbers to commit much larger crimes. The following sections look at some of these bigger scams.

### ***Credit Card Fraud by Botnet***

A botnet is a network of remotely controlled computers, usually meant for malicious purposes. To create a botnet, a person or an organization covertly installs malicious software on thousands or hundreds of thousands of computers, without the knowledge of the computer owners. The

## Chapter 10

### Credit Card and Epayment Scams

computers may be located in homes, workplaces, retail stores, government facilities, even IoT devices—pretty much any device that has an internet connection.

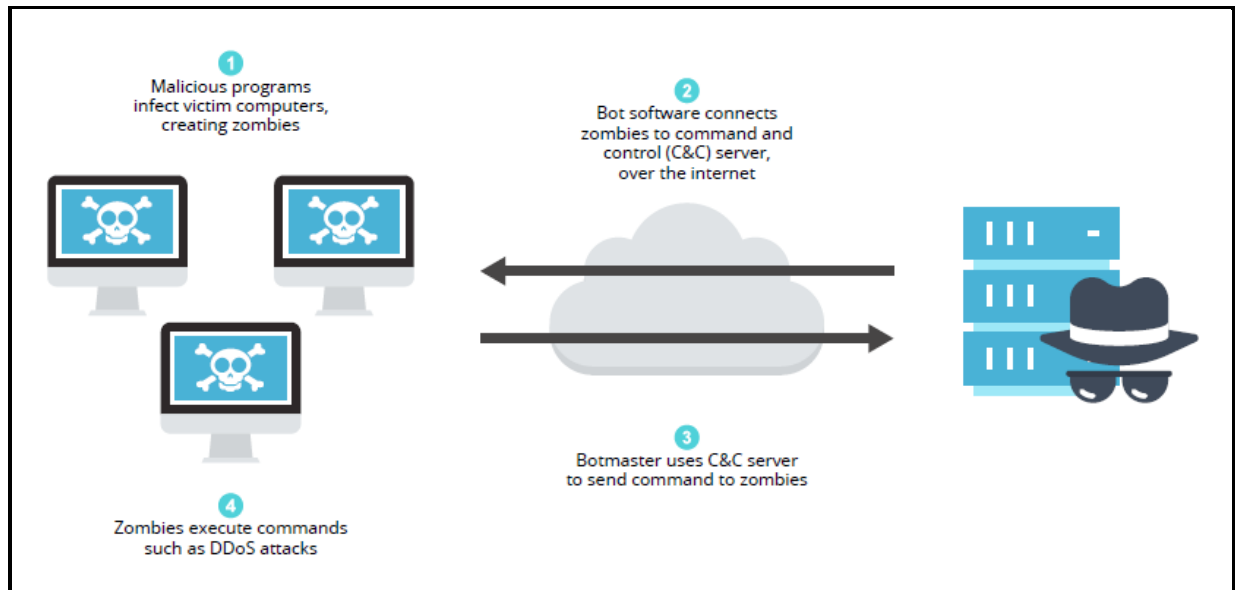
*The average-size botnet is around 20,000 computers. The largest botnets (as of 2017) were the Marina Botnet with 6 million machines, Conficker with 10.5 million machines and Bredolab with 30 million computers. [39] An even larger botnet known as Storm was estimated to consist of anywhere from 250,000 to 50 million computers. [40]*

Compromised computers that form a botnet are called **zombies**. These computers may be compromised because their owners click on links and open attachments, don't use antivirus protection, their systems are not up to date on security patches, or their antivirus applications are not kept up to date. Owners of zombie computers usually don't realize that their computers have been compromised.

The malicious person in charge of a botnet is known as a **botmaster** or botherder. You might hear news stories of how a botmaster used the collective power of thousands of computers to launch a distributed denial of service (DDoS) attack against a web server. Such an attack prevents anyone else from accessing the website associated with the server, essentially cutting it off from the world temporarily. Figure 33 shows the steps of a typical botnet.

A botnet can also be used to commit credit card fraud. A botmaster leases access to part or all of a botnet to a criminal organization. Those criminals then make a large number of fraudulent purchases from many online vendors over a short period of time. The use of the botnet hides the true location of the fraudsters, which is often in a country known for issuing massive amounts of spam. Botnets can create the illusion that they're in the same location as the owner of the stolen credit card number.





**Figure 33** A typical botnet usually includes thousands or hundreds of thousands of computers

## **WARNING!**

*Thanks to botnets, thousands of fraudulent purchases can take place with hundreds of online vendors simultaneously.*

### **An Example of Botnet Theft**

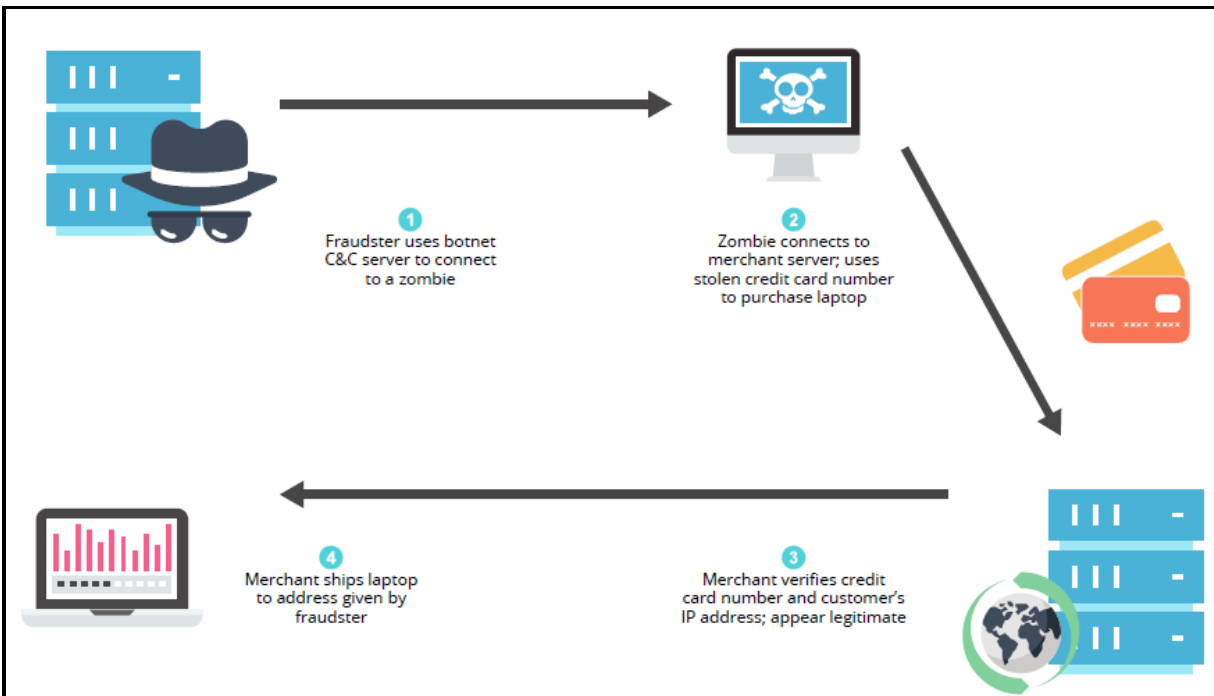
Let's look at the simple example illustrated in Figure 34. A fraudster comes into possession of one or more stolen credit card numbers. He or she logs in to a computer in Russia, for example, with an Internet Protocol (IP) address issued by a Russian internet service provider (ISP). If you could detect the IP address assigned to that computer, you could trace it to a block of addresses associated with the fraudster's true location.

The fraudster accesses a zombie computer in the same area of the United States as the owner of the stolen credit card number. The fraudster then uses the zombie and the stolen credit card number to purchase an item from an online merchant. The item is something that can easily be resold, such as a laptop. The merchant receives payment for the item using the stolen credit card.

## Chapter 10

### Credit Card and Epayment Scams

The merchant might use a fraud-detection application to verify that the IP address of the customer's computer is in the same general location as the credit card owner. However, because payment is being received through a zombie machine, the general location of the credit card owner and the computer owner appear to match.



**Figure 34 A simplified example of using a botnet to commit credit card fraud**

The merchant approves the payment and sends the item to the shipping address the fraudster specified. The item ends up in the hands of the fraudster or an associate and is sold in a foreign market. At some point, the actual credit card owner may notice the purchase of the item on his or her statement and notify the credit card company and the merchant. The credit card owner, the bank, and the merchant are all victims of this fraud.

Because a botnet can be composed of hundreds of thousands of compromised computers, fraudsters can commit fraud on a vast scale. All the while, they appear to online merchants as valid customers using U.S.-based computers. However, they are actually in a different location, using spoofed email addresses and stolen credit card numbers. Merchant losses can escalate into millions of dollars in a short time.

*Instead of using a botnet, a fraudster may use **proxy servers** to disguise his or her identity. A proxy server is a device that, for the sake of this example, operates on the internet using an IP address issued by an ISP in the United States. From the merchant's point of view, the proxy server represents the actual location of the customer. But the fraudster uses the proxy as a "mask" to hide his or her true location. The result is the same as if the fraudster had used a botnet.*

## Department Store and Private Label Card Fraud

The example of credit card fraud previously cited what is called "open loop" cards. These are cards you can use to purchase goods from a variety of merchants. They are the familiar VISA, MasterCard, and American Express cards. Department store credit cards and prepaid gift cards are referred to as "closed loop" cards because you can use them to purchase goods only from the issuing store. Despite the limitations of closed loop cards, criminals successfully use them to victimize merchants and customers.

### Department Store Credit Card Fraud

Fraudsters may use social engineering techniques to target customer service employees in a department store. The thieves convince the employees to release enough customer credit card information to allow these criminals to fraudulently purchase merchandise from the victim stores. Merchants can be any department store, including brands such as Best Buy, Home Depot, Lowe's, Macy's, Nordstrom, and Walmart.

The goal is to convince credit card customer service employees to either add a fraudster as an authorized user on the card or to change the authorized user from the actual customer to a fraudster. Individuals known as "runners" physically appear at the various department stores and verify that they were authorized users on the specified cards. The fraudsters typically use the cards for high-end purchases, including big-screen TVs, stoves, snow blowers, and large appliances.

### Gift Card Fraud

Several scenarios can be used to perpetrate gift card fraud. The most common is employee-driven fraud. Store employees can use different methods to commit gift card fraud. The method they choose is based on their access to these cards and the card activation process. For example, a fraudster may simply write down the card numbers of gift cards that are for sale and then use

## Chapter 10

### Credit Card and Epayment Scams

the store's website or toll-free number to find out when the cards have been activated. The employee can then quickly use the card number to make purchases.

Sometimes, an employee working as a clerk takes a gift card from a customer who is making a purchase. The clerk then debits the card for the purchase. The card still has a balance on it, so the clerk keeps that card and returns an empty, look-alike card to the customer. The employee then uses the customer's card to make additional purchases until the balance is drained.

Some store employees "clone" gift cards by using gift card numbers. When the card is activated by the customer, funds are loaded onto the cloned card rather than the customer's card.

---

*You'll learn more about gift card scams in Chapter 13.*

---

## PayPal Scams

PayPal is a highly reliable method of sending and receiving payments between individuals and organizations that might not otherwise have a common financial exchange method. Millions of people use it. However, PayPal is as subject to fraud as any other financial institution.

Fraudsters attack both individuals' and organizations' PayPal accounts. One common attack method is to use phishing or similar social engineering schemes. This fraud scenario is very much like other phishing scams. A person or an organization receives an official-looking email from PayPal, reporting a problem with the customer's account and asking the customer to reply to the email with his or her PayPal account information.

Phishing involving fraudulent PayPal emails can be a bit tricky. Unlike some other financial institutions, PayPal does send unsolicited emails to its customers. However, PayPal usually addresses the content of the email to the customer specifically, such as "Dear John Doe." Scammers typically address their emails as "Dear PayPal Customer" or something similar. These bogus PayPal emails are sent out to thousands or hundreds of thousands of email accounts, even to recipients who have never used PayPal.

PayPal customers who fall for the scam and give their account credentials to the criminals may find the bank accounts associated with their PayPal accounts drained quickly.

Fraudsters also use their access to stolen PayPal accounts to defraud other individuals or organizations. For example, say that an individual advertises an item for sale through an online outlet such as Craigslist. A fraudster sends an email to the seller, expressing interest in buying the item and asks to send payment through PayPal. The seller uses his or her existing PayPal

account or creates one, receives the payment from the buyer (but from the compromised account), and ships the item. One of two things will occur at this point:

- ✓ The actual PayPal account owner is out the funds for the item.
- ✓ The actual PayPal account owner revokes the payment after the seller ships the item, saying the transaction wasn't authorized.

In either case, someone has been victimized. This sort of scam also works at the organization level if the organization uses PayPal for any of its transactions. Employees who are responsible for authorizing PayPal transfers are just as vulnerable to social engineering scams as other people, and their computers can be infected with keylogger software to collect PayPal credentials. Sometimes, for example, European companies hire contractors in the United States to perform a service. Having no common financial payment method, the European companies use PayPal to transfer monies owed to the contractor. Robbing a private citizen's PayPal account usually won't yield very much money. However, if a fraudster gains access to several corporate PayPal accounts, his or her income could skyrocket.

## *Understanding Scamming Mechanisms*

Although the fraud methods used in the examples presented in this chapter vary, most of them rely on some form of phishing scam, at least in part. Numbers for customer credit cards, gift cards, and PayPal account credentials can all be acquired through some type of social engineering method. The defense against such attacks is proper education for individual consumers and corporate employees.

Highly organized criminal groups typically, but not always, operate elsewhere but victimize online merchants in the United States and Canada. Their success in perpetrating large-scale, very profitable fraud is based on the ability to steal large numbers of credit cards through a variety of means. They also depend on other criminal elements to create malicious programs to form botnets. As you've learned, cybercriminals use botnets successfully to commit wide-scale fraud against numerous online vendors, stealing millions of dollars' worth of merchandise, and then fencing or reselling said items in foreign markets.

Although criminal organizations can perpetrate department store credit card and prepaid gift card fraud, the most common scenario for this sort of scam is "the inside job." Store employees are well placed to commit such fraud because they have access to gift card numbers and the card activation process. Also, stores freely allow anyone to find out when a particular card has been activated via their website and a toll-free number, with only the card number that is visible right on the card. Non-employees can also commit similar acts of fraud if they have a method of knowing specific gift card numbers, such as stealing the cards from the store, scraping off the protective coating covering the card's number, documenting the number, recovering it so it looks

## Chapter 10

### Credit Card and Epayment Scams

untouched, and secretly returning it to the store where it can be purchased and activated by a legitimate purchaser. The fraudster will frequently check to see when the card is activated and immediately use it to drain all funds before the legitimate owner has a chance to use it.

PayPal, like any other financial institution, is vulnerable through its customers when fraudsters use social engineering to acquire account access information. While defrauding individuals yields limited rewards, the fact that organizations also use PayPal for payment transfers at an increasing rate allows fraudsters to access larger bank accounts and to acquire more stolen funds. There is some protection provided, although many exceptions to that protection exist, particularly for organizations with addresses outside of the United States.

To find out more about PayPal's rules for sellers, search for "seller protection" on the PayPal website. The Seller Protection web page outlines the specifics and offers a link to more detailed information. Similar information is available to buyers on the PayPal Purchase Protection page.

#### ***The Thing About PayPal***

*PayPal's Buyer Protection policy is available to assist customers who believe they are victims of fraud, but in PayPal's User Agreement under Miscellaneous Disclaimers, PayPal clearly states that it will not be held responsible for any fraud or deception by any user, whether or not they are a verified user. However, in the same agreement, PayPal states that after a payment has been made, the customer has up to 60 days to request a refund. Even so, the wording in the agreement indicates that PayPal doesn't guarantee that the payment will be reversed.*

*PayPal's Buyer Protection and Seller Protection policies are in place to protect both parties in a transaction from fraud, but they apply only to physical, tangible goods and not to items transferred electronically, services, quasi-cash, or any non-physical item.*

*PayPal's history of reimbursing fraud victims is not entirely clear. However, as reported at [www.steelesettlement.com](http://www.steelesettlement.com) in 2008, a class-action lawsuit was filed against PayPal and eBay, Inc., alleging that PayPal's policies and practices constituted deceptive trade practices. The lawsuit also alleged that a breach of the PayPal User Agreement occurred when PayPal customers who had been defrauded were not refunded their money. PayPal and eBay agreed to settle, and the final court approval of the settlement occurred April 30, 2009. Final payouts of the settlement were made on June 3, 2011. Another settlement has been proposed, according to [topclassactions.com](http://topclassactions.com), for active account holders between April 19, 2006 and Nov 5, 2015 to resolve allegations of improperly handled disputed transactions. This settlement was preliminarily approved on Nov 5, 2015.*

## *How to Avoid Card and Epayment Scams*

Avoiding fraud committed by large-scale criminal organizations using stolen credit cards and botnets or proxy servers can be particularly difficult. A number of enterprise-level antifraud solutions are available, but none of them have been found to be flawless. Also, even highly reliable antifraud solutions, if their technology does not continue to develop to match or surpass high-tech fraud methods, can quickly become ineffective.

Another difficulty related to choosing an antifraud solution is that many such applications offer a single technology that can identify only one type of fraud attack or one element that comprises a fraud attack. This is like a scientist wanting to analyze all the radiation coming from a distant star, but using a single telescope to accomplish the task. The telescope can detect only visible light, which makes up a small fraction of the total amount of radiation emitted by a star. The true solution is to employ a detection method that uses multiple devices together to gather the total amount of information the star generates.

Any effective antifraud application must either aggregate the solutions provided by multiple antifraud vendors or must offer, within a single platform, a suite of multiple technologies in order to provide a comprehensive service. Vendors such as Kount.com, iovation.com, and LexisNexis.com provide these types of antifraud solutions. Besides the effectiveness of the antifraud platform, cost is a deciding factor when measured against losses and potential losses to fraud. This is a significant consideration for smaller online vendors who might not have the budget to implement antifraud tools.

Because the majority of department store credit card and gift card fraud is associated with acquiring card numbers and is related to either employees being duped by fraudsters or employees committing the fraud, there are two solutions to consider:

- It's critical to train store employees in social engineering scams so they don't reveal even partial customer account information and do not add unauthorized persons to a customer's account.
- Guarding gift card numbers is especially important. Some stores have taken steps to sell gift cards in sealed containers so that only the customers can access the number after the purchase. This also thwarts casual thieves who "shop" for gift card numbers displayed in publicly available racks. Others store gift cards behind the counter in a locked cabinet.

PayPal takes steps to inform customers of how to avoid fraud by offering advice on its website, but the advice is the same advice you've read elsewhere in this book regarding phishing, vishing, and other social engineering scams. Also, frequent monitoring of banking and payment accounts

## Chapter 10

### Credit Card and Epayment Scams

can allow companies to quickly realize when fraud has taken place, allowing them to stop or revoke payments and to notify law enforcement agencies.

## *Chip and Pin Cards*

On October 1st, 2015, point-of-sale machines were required to accept “chip cards” (also known as “Chip and Pin” or EuroPay Mastercard VISA (EMV)), which are credit cards containing an embedded computer chip, and which may require a PIN, instead of a signature, to complete a transaction. Some issuers are using “Chip and Signature” cards, which also include a chip but require a signature instead of a PIN. In the U.S., most vendors don’t require a PIN or a signature for most low-dollar transactions.

As of October 1st, the liability for card-present fraud shifted to whichever party is the least compliant with the EMV standard. This means that if the merchant allows card transactions using the card swipe, they will be liable in case of fraud instead of the bank.

\*\*\*

All vendors that accept credit cards, especially online, are targets for merchant fraud. No fraud-detection service is perfect, although they can help with the problem. SME’s are especially vulnerable because they often cannot afford that kind of protection. Organizations of all sizes are at risk and businesses much be aware of the problem and take the appropriate steps to protect themselves.



# Chapter 11

## Mortgage Rescue Scams

“A man’s house is his castle.” This famous quote came from Boston attorney James Otis as he argued against “writs of assistance,” or warrants to invade and search all buildings suspected in smuggling, including a person’s home. Otis’s argument was that a man’s home is a secure and private dwelling, different from any other building. That was over 250 years ago, but it still reflects how we feel today: We need to feel secure about our homes. That’s why a mortgage rescue scam can inflict the most painful and cruel outcome of all scams.

In this chapter, you’ll find out what types of **mortgage rescue scams** exist, understand why these scams are more popular today than ever before, and learn how you can avoid becoming a victim. While mortgage rescue scams affecting homeowners are more prevalent than those aimed at organizations, a business mortgage holder can get duped as well. Predators out there are trying to scam organizations in almost the same way they’re scamming private homeowners.

### *A Sampler of Recent Scams*

A sense of security quickly fades when a business owner’s cash flow recedes or a homeowner is under extreme financial pressure. Those owners may be tempted to accept help to “rescue” their mortgages.

The mortgage rescue scam is fairly simple and has only a few variants. In all cases, distressed owners reach a similar outcome: They face steep financial losses and may even be losing their property. This section examines common mortgage rescue scams so you know what to watch out for.

#### ***The Phantom Help Scam***

In the **phantom help scam**, the scammer gains your confidence and an upfront payment, promising to act with the lenders on your behalf to rescue your mortgage. The phantom scam is so named because you believe the rescuer is helping you, but the scammer is simply lying in the shadows, doing nothing.

This scam works best when foreclosure is imminent—when you’re at the point of “too little, too late.” With little time left and no action on the part of the scammer, the foreclosure carries on. The scammer gets a great payment for almost no effort except a sales pitch.

## ***The Bailout Scam***

Like the phantom scammer, the **bailout scammer** exerts little effort, but for a much larger gain: your house. In the bailout scam, the scammer promises to bail you out of your obligation to the lender. The scammer's main promise is to stop the foreclosure immediately. You sign a document that allows the company to act on your behalf with the lender. Other promises might include helping you recover your credit score and get back into good standing with your lender.

For example, after a review of your situation, the scammer may offer to take temporary ownership, with an arrangement to retain you as a renter. Naturally, the scammer insinuates that you'll be able to purchase back the house after everything is squared away. In reality, you sign over the house and lose whatever equity you had to the scammers. If you opted to rent, you would find it too expensive because the scammer makes it unaffordable in order to have you evicted.

## ***The Bait-and-Switch Scam***

The **bait-and-switch scam** is like the bailout scam, only more sinister. The scammer does help bail you out of your property, with a promise to help you save or recover it after a short period. The pressure is high to sign a tempting agreement for a new loan or new terms. Instead, you sign over the property title to the scammer, transferring ownership. Although some documents may be forged or fraudulent, the scammer still receives actual ownership.

In many cases, the victim ends up with no asset but keeps all the liability. The scammers say they want to bail you out of your obligation to the bank. All they really do is bail you out of your property. When the scam works and the property title is transferred, the victim is still left owing the mortgage. Ouch.

### ***Ripe Market = Rampant Mayhem***

*Following the economic distress caused by the COVID-19 pandemic, millions of people are having to make tough choices about which bills to pay, if they can pay any at all.*

*Foreclosure, the procedure in which a lender reclaims property to secure an owner's debt, is likely to become increasingly common. With the booming market of desperate homeowners, foreclosure scams are also increasingly common.*

*Difficult economic times cause increases in mortgage fraud, as was seen after the 2008 financial crisis. Organizations prey on desperate people, offering "mortgage modification" or "foreclosure assistance." These organizations use predatory tactics to entice homeowners to sign over their homes—without recourse.*

*As homeowners get scammed and report the scammers to watchdog organizations such as the Better Business Bureau (BBB), the number of complaints can become overwhelming. Some watchdog organizations have since started redirecting complaints to law enforcement agencies. Law enforcement is relatively inexperienced with such crimes and has little legal support because these types of crimes are too new for protective legislation to have passed. In short, the market has become ripe for mortgage scams, and there's little to no recourse except to exercise strong "buyer beware" awareness.*

## **Mortgage Escrow Fraud**

When you buy a home using a mortgage, the money or a fractional down payment is frequently required to be placed into an escrow account. This means that the payment is held by a third party until the transaction is complete and all the terms of the contract are fulfilled. Thus, when you purchase a home, you'll deposit your money into escrow, and it will be released to the vendor when both you and they have fulfilled any obligations. For example, the vendor might need to fix the roof or repair the plumbing; in this case, the money would not be transferred until those repairs were completed.

In **mortgage escrow fraud**, criminals trick you into transferring the money in the escrow to a fraudulent account. Sometimes this is done when the hackers create a fake website that looks very similar to the legitimate escrow site and sometimes they will email instructions to you to wire the money to them instead of the escrow. They could also email the title company to perform the same transfer. Once the money is in the hacker's accounts, they transfer it out and it's gone.

To protect yourself from this kind of scam, make sure you're working with someone directly at the title company. Meet with them or speak to them. Don't accept any unsolicited calls or emails regarding transferring your money. Most importantly, don't use the phone number or links within an email that you receive on the subject, even if you are expecting it and it looks completely legit. Instead, make sure you have the title company's correct phone number and use it to confirm the details of any transactions before transferring money.

## *Understanding Scamming Mechanisms*

It's important to be aware of how scammers prey on others and lure people to cooperate. Understanding their tricks and techniques should reduce your chances of becoming another statistic. Remember, "to be forewarned is to be forearmed." This sentiment applies to mortgage scams as well as all other scams.

Mortgage scamming tricks are simple but effective. Scammers rely on misinformation, pressure, and your lack of knowledge. Further, when you're desperate, their job becomes even easier.

## Chapter 11

### Mortgage Rescue Scams

A mortgage scam begins with an offer to help. You might receive an email with the subject line “Stop Foreclosure Now!” or “We guarantee to stop your foreclosure.” This creates hope and ultimately trust. With trust, your skepticism fades, even when the advice seems completely counterintuitive. The misinformation begins to erode your legitimate options, cutting you off from those who could truly help you. If the scammer is successful and applies pressure at just the right time, you and your property are separated.

### **Bad Advice**

Mortgage rescue scammers use a number of catchphrases to separate you from your property and money. Let’s look at them and examine why they’re the opposite of what you need to hear.

#### *“Let Us Help You”*

Whether you’re actually in trouble with your mortgage, would simply like to refinance, or are just interested in what they have to say, you call their number. A warm ear is all they need: someone who owns a house, a business property, or any other equity and is at least semi-interested. The scammer starts with “Let us help you” and invites you to a meeting. You’re hooked.

#### *“We Can Help You Start Over”*

At the meeting, distressed owners in particular hear exactly what they want to hear: You can start over, wipe the slate clean, forgive and forget, get back to square one—to where you were before your troubles began. Legitimate lenders don’t say such things, but the scammers are reeling you in quickly. They’re feeding you empty promises. However, when an owner is facing hard financial times, any offer seems worth a listen, even if it’s too good to be true.

#### *“Stop Talking to Your Bank”*

The rescuer advises the owner to stop communicating with his or her lender and any attorneys. Of course, this is the opposite of good advice. Once the owner refuses to cooperate with the bank, the bank interprets this as unwillingness on the borrower’s part to repay the mortgage or negotiate alternate terms. Foreclosure becomes certain, which is exactly what the scamming rescuer wants.

#### *“We Can Buy and Rent It Back to You”*

Scam artists offer to rescue the mortgage for the owner and then rent it back to the owner. If an owner chooses this option, the rescuer’s next step is to spike the rent so high that the owner will soon be evicted from the property.

#### *“We Will Cover Your Losses”*

Instead of renting it to you, the scam artist may offer you an exchange. In return for paying back all your missed payments, which will help recover your credit rating, the scammer takes any

potential gains from the foreclosure sale. A fraudster uses this scam only when he or she knows the home sale price will far exceed the current loan amount and delinquent payments.

### *“Transfer the Money”*

The scam artists ask you to send payment for a house controlled by the bad guys, based upon a spoofed (counterfeit) email from the “lawyer” involved in the real estate transaction.

### ***Casting for Leads***

*If you’re looking for phone numbers for scammers, you don’t have to look far. You can find scammer marketing on fliers, billboards, ads posted in the supermarket, classified sites such as Craigslist, and even hand-written notes left in your mailbox.*

*In the case of delivered mail or direct contact, you may wonder how the scammers find their information. There are companies that gather, assemble, and sell lists of individuals and organizations suffering with their mortgages. To scammers, such a list is a treasure chest full of qualified leads.*

*There are plenty of people having difficulty with their mortgages. Still, getting a hold of lists of targeted individuals saves scammers tons of time. On top of the money saved in blanket marketing, the revenue earned from realized scams becomes nearly 100% profit, with little overhead.*

## How to Avoid Mortgage Rescue Scams

The best advice for avoiding mortgage rescue scams is to avoid having to rescue a mortgage. Sadly, this isn’t always possible. If an owner faces mortgage payment difficulties, the first and best action is to speak with the lender about options. The options available depend on the lender and the owner’s payment history. Some examples include changing the terms of the mortgage, reducing payments temporarily, extending the loan period, and even allowing the owner to contribute a partial payment for an agreed period. Remember, owners aren’t the only losers in foreclosure. Lenders are likely to lose money when a property goes into foreclosure, so most lenders prefer to avoid it.

In addition to working with the lender, a homeowner should seek the professional help of a Housing and Urban Development (HUD)–approved counseling agency. When suffering from mortgage payment problems, it’s critical to contact a HUD-approved counseling agency before the foreclosure process begins.

*To find a HUD-approved agency in your state, visit [www.hud.gov/offices/hsg/sfh/hcc/hcs.cfm](http://www.hud.gov/offices/hsg/sfh/hcc/hcs.cfm) The advice is either free or very low cost. Plus, it’s always in your best interest.*

## Chapter 11

### Mortgage Rescue Scams

Even without financial resources to keep mortgage payments on schedule, owners who demonstrate good intentions for improving the situation may also improve their standing with the lender. Lenders consider all behavior, good or bad, when making decisions about foreclosure.

### ***Knowing the Vulnerabilities That Are Attractive to a Scammer***

If your mortgage is troubled, can you avoid mortgage rescue scams? Yes, but not as easily as you can avoid other scams. Most scams work on a vulnerability based on misplaced trust (such as checking the box to remember your password on a public computer) or something overly enticing (possibly too good to be true).

Both of these apply to mortgage rescue scams, but with a key addition: emotion. Your property is probably the largest asset you possess. With a mortgage, be it on your home or organization, you're emotionally involved. With a troubled mortgage, you're often desperate and extra willing to place trust in someone or something glaringly wrong.

### ***Seeking Professional Help***

Consumer protection and business attorneys as well as real estate attorneys are the legal representatives best suited for fighting foreclosure. Most distressed owners are strapped for cash, so incurring additional fees might seem counterproductive. However, a hired professional will ensure that the procedures followed protect your best interests.

Even before you hire an attorney, the following section provides invaluable advice to ensure that you avoid mortgage rescue scams and behave most effectively to save your mortgage.

### ***Understanding What to Do and What Not to Do***

Let's start with actions distressed owners should take:

- ✓ **Take stock of your situation:** Determine whether you're close to foreclosure or only behind in payments. Receiving a deficiency notice (because you're behind on one or more payments) is far better than receiving a notice of a trustee's sale (the date is set for public auction of your property). If you're experiencing only a delinquency, immediately act to resolve the debt.
- ✓ **Acquaint yourself with the laws in your area:** Every state's laws are different regarding rights and timelines.
- ✓ **Choose a legitimate attorney or other counselor:** It's important to seek professional and relevant counsel. Ensure that the person or company you want to work with is certified by HUD ([www.hud.gov](http://www.hud.gov)) to avoid another scammer. You shouldn't have to pay for legitimate housing counseling.
- ✓ **Communicate:** Be cooperative with the lender or counsel representing your lender.

- ✓ **Don't respond to unsolicited emails or pop-up ads:** Steer clear of unsolicited emails and pop-up ads online that promise to get you back on track. Falling for such tricks is likely to put you in more trouble than you already face.

Now let's look at some don'ts:

- ✓ **Don't avoid the problem.** Procrastination is a sure way to lose.
- ✓ **Don't rely on oral agreements.** Any offer should be in writing, and you and your source of professional help should review it carefully.
- ✓ **Don't be pressured into signing anything before you review every document fully and with professional help.**
- ✓ **Don't surrender principal or interest payments to any entity outside your lender, no matter how "direct" the relationship seems.**
- ✓ **Don't agree to rent the property and possibly buy it back later.**
- ✓ **Don't sign a home-sale contract if such a contract doesn't release you from your existing mortgage.**
- ✓ **Don't sign a quit-claim deed unless your attorney tells you to do so.**

## Wrapping Up

In this chapter, you learned how mortgage rescue scams can negatively impact homeowners and organizations. You got a sense of how current economic conditions, lack of legal recourse, and human emotions all contribute to the surging market for mortgage scammers. You examined how some common mortgage rescue scams work and picked up tips for protecting yourself from scammers. You also learned several actions to take (and not to take) if you find yourself needing help.

### ***Foreclosure Fraud: Official and Systemized***

*For a few years, avoiding foreclosure fraud wasn't as easy as simply being aware and taking cautious steps around individual scammers. In some respects, foreclosure fraud was systemized by the complex mortgage securitization chain of servicers and trusts. This fraud was made possible by forged documents, electronic processing where signed documentation is legally required, and systemized verification ("robo-signers"). While certainly a different scenario than scammers operating as rogue companies, the reputable companies systemizing the disenfranchisement of owners may be considered fraudulent as well.*

## Chapter 11

### Mortgage Rescue Scams

*Mortgage-related fraud has garnered much press over recent years, but only recently has it been scrutinized. Still, it has affected those who make all their mortgage payments on time—and even those who don't hold mortgages. Systemic fraud is now being investigated. We can expect lawsuits from disenfranchised homeowners and organizations to surface for years to come.*

\*\*\*

In summary, here's what you need to remember:

- ✓ Work with and make payments to your lender. Avoid dealing with anyone else.
- ✓ If someone advises otherwise or is acting as an “approved/government” entity, run. If something sounds too good to be true, it is, especially when it comes to your mortgage.
- ✓ Act objectively. Take action with as rational a frame of mind as possible.



# Chapter 12

## Automated Clearing House Scams

Automated Clearing House (**ACH**) is an electronic network that banks and other financial institutions use to conduct transactions. These transactions use information found on business and consumer checks, normally authorized by that organization or consumer. The transfer might be a single or recurring debit to their account. ACH scams are unauthorized debits to drain money out of accounts.

In this chapter, you'll learn why ACH scams exist and how they've become popular both online via ecommerce and offline. You'll find out what makes some organizations easier targets than others and why. Finally, you'll learn steps your organization can take, both technical and nontechnical, to nearly eliminate your risk of losing money to ACH scam artists.

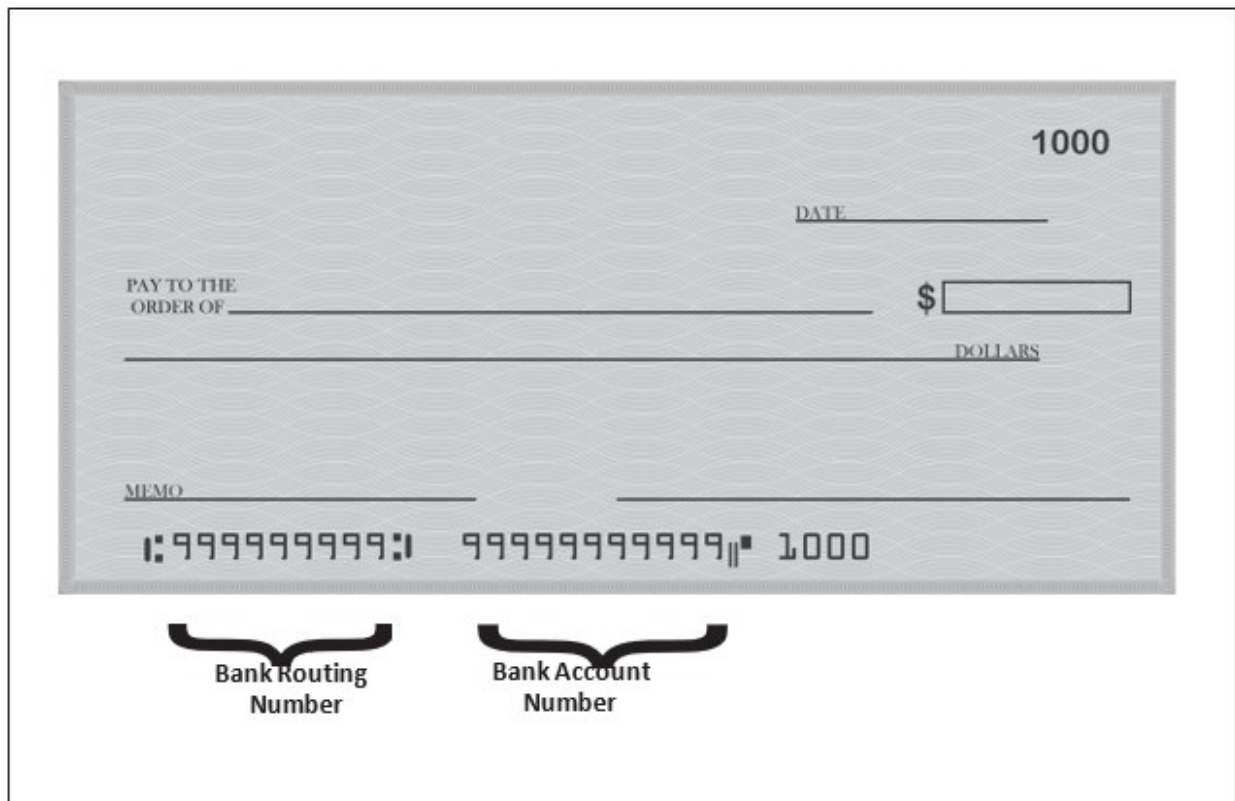
### *The Most Lucrative Scam Against Organizations*

Organizations of all sizes use ACH to conduct financial transactions in the United States. When your organization makes direct deposits for payroll or issues recurring payments such as for a monthly lease or utilities, you're likely using the ACH network.

An ACH transfer, whether it's a deposit or a debit, requires two numbers: the bank's routing number and the customer's account number. These two numbers, found at the bottom of every business and personal check (see Figure 35), are used to initiate a transfer from the payer's account to the recipient's account. This transfer occurs electronically, using the ACH network.

## Chapter 12

### Automated Clearing House Scams



***Figure 35 Location of bank's routing number and account holders bank account number on a typical U.S. check***

Sending money electronically is a fantastic evolution in doing business compared to having to visit a teller window for each transaction. However, removing the teller window also removes the bank's ability to verify the customer's identity. Without physical presence at a bank, a customer and someone posing as the customer appear equally qualified to initiate a transfer. This is the main vulnerability that enables ACH scams to flourish.

### ***How Big Is the Score?***

The amount an organization or an individual can lose depends on the available balance in the owner's bank account. The more money available, the more the scammer can grab. However, the scammer usually won't send all funds in one transfer or to one account. Instead, the scammer depletes the account by several, smaller transactions. Transactions for organizations are typically about \$9,000, and rarely above \$10,000, for reasons explained later in this chapter.

Despite the relatively low transfer amount, this type of crime can be massively profitable. A 2020 report from JP Morgan [41] found that 81% of organizations were hit with payment fraud. Only

a relatively small portion of losses are recovered because the scam works so well. And these are the losses law enforcement has identified; they're likely just the tip of the iceberg.

## Targeting Objectives and Requirements

ACH scammers are becoming more discerning than the average phisher and now often target certain types of victims rather than spamming the masses. For ACH scams to be successful as often as possible, a criminal must have the ideal victim in mind. Here we look at characteristics that define the typical victim of an ACH scam.

SMEs, which include small companies, nonprofits, schools, and other public institutions, are the common targets of **ACH scams**. Why? Compared to most families, SMEs experience larger, more frequent cash flows. Also, SMEs do not have the sophisticated finance departments that are common in larger corporate environments. Going further, a corporate firm would have several layers of controls in place in its accounts payable department, making a rogue ACH transfer more readily detectable.

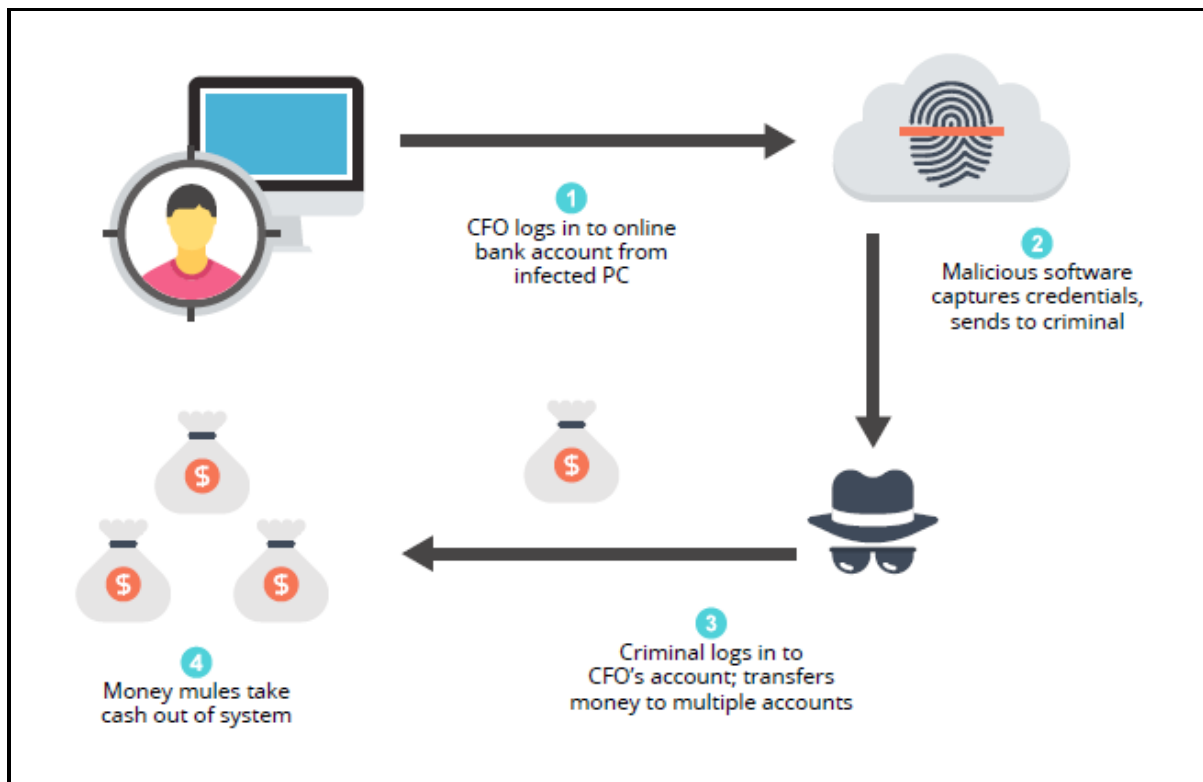
Finally, targeted SMEs are likely to deal with local or community banks and credit unions. The advantage to defrauding accounts in a local community bank is that the ACH transactions are normally handled by third-party service providers.

### ***ACH Scammers Like PayPal, Too***

*ACH scams are not restricted to checks and interbank transactions. In creating a new account with PayPal, for example, a user must provide his or her credit card number and checking account information. This means entering the routing number and account number found on checks. In short, PayPal is able to use the ACH network for online purchases, making the user vulnerable to ACH scams. Of course, this is not restricted to PayPal, as many online merchants permit ACH debits as a form of payment.*

## An Example of a Basic ACH Scam

ACH scams follow a known series of steps. An example of an ACH scam is shown in Figure 36, but the actual steps are more complex. Having an understanding of these steps empowers you to be more aware and more adept at protecting yourself and your organization. With each step described in the following sections, consider your own organization's vulnerabilities and strengths as a potential target.



*Figure 36 An ACH scam in action*

## **Scouting for the Right Spot**

Criminals, no matter how well funded, like to go after easy prey. Anyone who has hunted or fished knows that having the right equipment serves no value if you're in the wrong field or stream. Earlier in the chapter, we profiled types of ACH scamming prey—small businesses, nonprofits, schools, and other public institutions. But even among these common targets, a scammer looks for particular characteristics.

An organization that appeals to ACH scammers advertises the contact person of interest—that is, the person handling funds for the company. Criminals most appreciate an organization that publishes the organization chart on their website. One look on a public website can yield the chief financial officer (CFO) or other person who handles financial disbursements. If the person's e-mail address is also given, that saves yet another step.

## **Casting the Lure**

The next step in an ACH scam is to get the contact person to click to open and install some malware on his or her computer. One example, ironically, is to press a button or link that

promises computer security. In most workplaces, the operating system used is some Microsoft Windows variant. Therefore, a well-drafted email alerting the CFO of a critical Microsoft patch may get the required mouse click, especially if the message is spoofed, appearing as if it's from the CFO's own internal IT department.

If the CFO clicks as instructed, he or she will visit a rogue website that may appear to be the site of Microsoft, a local bank, a social network site, or some other "trusted" site. The malware posing as a security patch, a bank statement, or something personal is now installed. The computer is now running a Trojan program that includes a keystroke logger, waiting for the next time the CFO logs in to the bank's website. During the next login, the malicious software captures the CFO's credentials and passes them on to the criminal in the background. The CFO leaves the website and carries on with business, none the wiser.

### ***Jumping Ship***

The criminal now has the username, password, and any other captured credentials the CFO used to access the bank account. The criminal can immediately log in and initiate a transfer directly. Money is transferred out of the account and distributed to several other accounts, seemingly at the command of the organization's CFO.

### ***And Like That—Poof!—The Money Is Gone***

At this point in the ACH scam, the criminal has used the newly gathered credentials to distribute ACH transfers to several accounts. These accounts are likely newly created just for the sake of receiving these funds. There's no reason to believe the accounts are geographically near the victim, or each other, or even in the same country.

Each transfer is likely right around US\$9,000. This is because any U.S. bank that transfers amounts over US\$10,000 is legally required to submit a currency transaction report (CTR) due to anti-money laundering legislation passed in 1986. Today, banks have systems in place that automatically send a required CTR, so a fraudulent ACH transfer stays below that threshold to avoid the alert. To transfer over US\$10,000, all the criminal must do is distribute the total balance via multiple transfers to multiple accounts. And of course, scammers do this—until the victim's account is completely drained.

### ***"Mules" Willing, Waiting, and Able***

Who collects the money in an ACH scam? The collectors are people who were recruited to quickly receive and turn around the funds to the criminal organization, often unaware of their actual role.

## Chapter 12

### Automated Clearing House Scams

To law enforcement, these people are known as money mules. Whether unwitting or willing, these mules immediately withdraw the distributed funds as cash. The mule then wires the cash to places like a Western Union or MoneyGram office, usually in Eastern Europe, where it's finally collected by the criminal organization. Money mules serve as an interrupt to the electronic process. This interrupt stops law enforcement from possibly knowing which Western Union office the money was routed to without finding and personally interviewing each mule. By the time the law catches up with a mule, the money is long gone.

Money mules are recruited in several ways, but most popularly through online "work from home" ads or through responses to their resumes on employment sites. Mules receive instructions through a manual written by the criminal organization. These instructions provide a full background ruse, keeping the mule unaware of the actual scam. As payment for their services, mules keep a nominal amount or percentage, as instructed.

### **Trojan Not Required**

Using the ACH network for unauthorized transfers can be far easier than the process just described. Instead of targeting a specific person, planting Trojan software, and using captured credentials, a criminal can simply abuse a legitimate relationship between organizations.

Let's say an organization provides account information—that is, business account and routing numbers—by way of a check payment. The payment was intended to be a one-time charge, but the check's recipient still has the opportunity to continually make charges against the account. Obviously, once discovered, these unauthorized transfers could severely damage the relationship. But for some, it may be worth damaging relationships in this way.

#### ***The Consumer Angle: ACH Scams Using iTunes and PayPal***

*Reports to the FBI show that ACH scams are growing in frequency and scale. As the growing popularity of online business and payment methods grows, so does the potential for scamming consumers and organizations.*

*Take the case where customers of iTunes, Apple's popular online music and media store, saw their bank accounts depleted due to unauthorized iTunes purchases. Each victim had a direct connection between his or her iTunes account and bank account, via PayPal. Users cried foul to Apple, blaming a security breach in the company's iTunes store. In opposition, Apple noted that each user fell victim to emails that led to scammers compromising their accounts. In the end, the connection between iTunes and PayPal accounts on the users' computers was the vulnerability that allowed unchecked ACH debits to the point of completely draining personal bank accounts.*

## *Occasional Scam Elaborations and Distractions*

Earlier in the chapter, we looked at how a typical ACH scam works. But some scam artists might take extra steps. Taking extra steps can boost the scammer's chances of avoiding detection or thwarting a victim's attempts to recover the funds—even if it also means drawing large amounts of attention to the scam itself.

Consider an example that involved an ACH third-party provider. Remember that small, local banks often rely on ACH third-party providers for handling ACH transactions. (Large banks normally handle these transactions internally.) In this case, a criminal had taken the extra step of compromising computers of the ACH third-party provider. The scammer then launched a distributed denial of service attack on the provider immediately after funds were transferred to mules' accounts or pickup points. The DDoS attack was to prevent communications while funds were waiting for mules to collect them, lest the provider and bank try to recall the fraudulent transfers before cash was withdrawn. No doubt the attack brought on a lot of undue attention, but it did reduce any ability to possibly recover funds already stolen.

### **Distributed Denial of Service (DDoS) Attack**



A distributed denial of service (DDoS) attack is an extension of a DoS attack. However, while a DoS attack uses a single system to attack another, a DDoS attack employs several to hundreds of thousands of different systems. Using many systems for a DDoS attack can help ensure that communications are completely denied rather than disrupted to a lesser extent as a system might withstand a simple DoS attack. The largest DDoS attacks now can direct more than 600 Gbps (Gigabits per second) of fake traffic against a single computer or service.

## *How Fraud Detection Plays into ACH Scams*

First and foremost, detection and loss recovery hinge on timing. We discussed earlier that very soon after a fraudulent transfer is made, the funds are redistributed to various accounts, and mules are standing by to make the withdrawals. In some cases, accomplices are even waiting in line to receive cash while the phone is ringing to alert the cash desk of the fraud. But no one wishes for such “luck,” nor can they rely on it. Once cash exchanges hands, recovery becomes nearly impossible.

Detection and timing are key to reversing a fraudulent debit prior to cash ending up in the criminal's hands. In this case, detection means watching account activity constantly. Simply noticing suspicious transactions may be too little, too late. By the time a debit transpires, the

## Chapter 12

### Automated Clearing House Scams

criminal has already gathered the credentials, tested them for validity by logging in elsewhere, and performed some reconnaissance on the account.

Thankfully, today's technology permits monitoring not just transactions but also the behavior of viewing activity. For example, a bank may employ technology to monitor how often or how extensive a customer views their account. This establishes a baseline of the customer's behavior. Compared against an established behavioral baseline, a criminal's reconnaissance may trigger flags as "out of the norm." A simple email alert or text message can provide enough additional time to investigate further.

## *Avoiding ACH Scams*

Some of the best ways to defeat ACH scams involve having smart practices in place involving key people. In this section, we discuss a few tips that could benefit every organization.

### ***Increasing User Awareness***

When dealing with threats of any kind, ensuring that the people involved are aware of the threats diminishes the risk of being exploited. In short, people kept in the dark bump along blindly, while informed people can make informed decisions. This goes for all scams, including ACH scams.

Some may say that user awareness training educates the trainees with "how to" training. However, this is a myth—as long as the organization isn't providing step-by-step examples of how to commit ACH fraud. As part of awareness training, a user should get an overview of ACH scams, what conditions would invite such scams, examples of signs to watch out for, and, most importantly, what specific steps to take when suspecting an ACH fraud.

### ***Implementing Auditing and Controls***

Work environments typically have a single person in charge of some area or set of tasks. Keeping one person accountable for an area fosters productivity. However, it's important to implement independent auditing and controls to prevent abuse within such areas. This is especially true when dealing with ACH fraud that could potentially be controlled by a single person within an organization.

Whether an internal group or external entity performs the auditing, it is essential that the auditing be done independently from the department under review to ensure no conflict of interest or cover-up. In addition, having controls in place, whether technical or procedural, can provide checkpoints that also minimize the risk of abuse.



## **Reviewing Corporate Accounts Daily**

Best practice says we should review corporate accounts daily. Before delving into why, let's first consider how often we review our own personal accounts. How often do you reconcile your personal bank account? How often do you look through and resolve all the transactions? If you do it at all, you probably do it monthly, when you receive your statements. What happens when you discover a transfer you and your family members didn't initiate?

*Many banks allow customers to set "fraud alerts" for newly added accounts and large balance transfers. See if your bank has "fraud alerts", and if so, enable and use them.*

Say that you discover a very large withdrawal or a recurring debit that you're sure wasn't approved. Do you still have a chance to resolve this with your bank? Yes. In fact, even if you skip a month of reviewing your statements, you're probably safe. That's because banks offer a 60-day window in which personal account holders are not held responsible for fraudulent transactions. For up to 60 days, you can report fraud to your bank, and you're entitled to full recovery of funds as per the FDIC.

Does a corporate account also have a 60-day window to report fraudulent activity? Can it resolve a rogue debit with its bank if the debit is 59 days old? No. How about 14 days or even three days? No. Corporate accounts are responsible for ACH debits after only two days! An organization must therefore review its corporate accounts daily. Put it into practice, make it a habit, and save yourself the responsibility if or when a fraudulent debit occurs, because corporate accounts are not FDIC insured.

## *Technology Steps That Can Help Avoid ACH Scams*

An organization can take some steps to better defend against fraudulent ACH transfers and to detect them when they occur. The previous section covers critical nontechnical means of combating ACH scams, such as user awareness training and daily review of corporate accounts. Those precautions, however, should be accompanied by technical steps as well.

### **Implementing Defenses**

Using multiple layers of security is important. Much the same way a secure home employs a fence, door locks, and an alarm, an organization needs to employ layers of security for its banking. It should be obvious that access to bank accounts, whether direct or to privileged computers dealing with accounting, must use multiple layers of security.

### ***The Limitations of Antivirus Software***

*Even if all the computers in your organization have up-to-date antivirus software on them, it's still possible for them to get exploited by malware. Antivirus software provides nearly no protection against ACH scams.*

*Remember that these scams involve malware being sent to an internal computer, either by email or through a visited website. Experiences shared from law enforcement agencies and IT security companies reveal that antivirus software is declining in effectiveness against malware. Most antivirus companies require previously known malware to produce "signatures" for their software—hence the need to continually keep the software up to date as the list of malware variants grows. Unfortunately for us, the variants of malware distributed for ACH scams change far too rapidly for antivirus companies to stay on top of them all in a timely manner.*

*Virustotal.com is a website on which you can scan individual files or URLs with over 70 different antivirus engines at once.*

### **Diversifying Defenses**

When all the layers of security are confined to one communication channel or system, the security lacks the depth and complexity necessary to mitigate all theft. Say that a legitimate user must enter a username and password as one step, answer a challenge question as the second step, and then enter a personal identification number (PIN) as the final step—all on the same computer, at the same screen. How secure are those multiple layers of security when the user's keystrokes are being logged surreptitiously? How easy is it for a thief to record and steal all three steps of these credentials? What happens then?

Now, consider a scenario where the user must enter a username and password combination and then wait for a unique PIN to be sent via SMS (text message.) After entering that PIN, the user has access. The system has in fact only two steps of credentials, but it employs a different means—the user's mobile phone—to deliver the second credential. A thief would have to compromise both the computer and the user's phone to gain access, after having already stolen the username and password. Consider how much more secure this method is—and it uses only two forms of authentication rather than three! This type of defense is called **two-factor authentication** (2FA) or multifactor authentication (MFA)."

*It's helpful to analyze your organization's practices through the eyes of a thief by asking "what if...?" frequently. For example, ask yourself, "What if this password were compromised? Would someone need anything else in order to empty the account?" or "Are any safeguards in place in case our supplier double-charges us?"*

Bear in mind that users may not welcome adding technical steps for the sake of security. Some users may even seek to circumvent complex procedures if they don't understand why those procedures are necessary. But experience shows that users who appreciate the reasoning behind the technical steps are far more understanding of the added effort and will be less likely to circumvent it.

### ***Minimizing the Number of Accounts and Personnel That Permit ACH Transfers***

Earlier in the chapter, we discussed the importance of reviewing account transactions, especially in business accounts where the organization has only two days to alert the bank to problems. Reviewing business accounts daily can be a daunting task, depending on the number of transactions and accounts. A good technique for minimizing threats—and one that also makes reviewing easier—is to limit the number of accounts that permit ACH transactions. Similarly, limit the number of staff who are permitted to initiate and authorize ACH transfers. If an account is capable of allowing an ACH transfer, that account must be reviewed daily.

\*\*\*

Now that you've learned about ACH scams and how they can be used to steal from businesses, implement the appropriate policies, procedures, and training to fight back. This is one area where technical solutions are less effective than informed and diligent personnel.



# Chapter 13

## Retail Scams

Online retail is hot. Consumers and organizations are increasingly turning to their computers and the internet to buy products and services. During the 2019 holiday season, total holiday sales were US\$626 billion, online and other non-store purchases grew 4.1% to US\$730.2 billion [42]. That enormous amount of money provides plenty of motivation for retail scammers.

Unfortunately, from worthless gift cards to bogus promotions, the retail industry is hit with fraud at every turn. This chapter looks at several different kinds of retail-related scams, many of which are aimed at organizations. You'll find out why organizations make good targets and how potential victims are fighting back. You'll also pick up tips to protect you and your employees from falling for such scams.

### *Bigger Organizations Attract Criminal Attention*

Sophisticated cyberthieves are targeting organizations more and more these days, mainly because the payoffs are big. Business accounts usually have higher credit limits than consumer accounts, and organizations generally make bigger purchases. It's often easier for fraudulent charges—even relatively large fraudulent charges—to sneak by personnel in a busy purchasing department than to slip past an individual who's watching every penny.

The total losses to fraud throughout the U.S. now average US\$170 billion a year as of 2019, according to Frank McKenna, the Chief Fraud Strategist for AI firm *Point Predictive*. [43] That is roughly 1% of the GDP of the United States.

#### ***The Innovative Cybercriminal***

*Attendees at an internet retailer conference in Boston took part in an informal survey regarding online fraud. When asked who's winning the war on fraud, one responder wrote: "Nobody wins—the best we can hope for is a draw." It was an insightful response. Cybercriminals constantly find new ways to improve old scams and use new technology to create even better and more successful scams.*

## A Sampler of Recent Scams

Let's look at some of the retail scams that are proving lucrative for thieves. These are the types of scams you and your employees are likely to encounter, including gift card scams, promotion/discount scams, and bogus account credit scams.

### Gift Card Scams

Gift cards are a multi-billion-dollar industry at US\$171 billion in the U.S. in 2019 [44] and \$619.25 billion worldwide. [45] So, it's not surprising that gift card scams are alive and well.

There are two main types of **gift card scams**: those that target cards you buy at a brick-and-mortar store and those that arrive by email or the web.

#### Brick-and-Mortar Store Scams

In a store, retailers most often display gift cards on a rack. A crook can easily jot down card numbers and the toll-free numbers found on the back of cards or scan the magnetic strip on the card with a portable scanner. Then, all it takes is dialing the toll-free number every day or two, entering each card number, and checking the balance. Once a customer buys a card and loads it with money, and the salesclerk or customer activates the card, the crook can quickly use the card to shop online, draining the balance in minutes.

## WARNING!

*Fancy gift card packaging doesn't always thwart a crook. Depending on how a card is packaged, a scammer can carefully pry the gift card out and then put it back after stealing the concealed numbers.*

Retailers must also keep a close eye on salesclerks. A deceptive clerk might keep a stash of used, inactive cards at the register. When a customer buys a card, the clerk takes the payment, activates the new card, and hands a worthless card back to the customer. Or, when a customer attempts to use a gift card, the clerk may pretend the card has no balance and offer to throw it away. After the customer leaves, the clerk slips the card into his or her pocket and shops online later.

### ***The Social Engineering Side of Gift Card Scams***

*With a rogue clerk at the checkout stand, the odds are stacked against the customer. If a customer has made other purchases on a gift card and is subsequently told that the card has a zero balance, the customer may assume that the card balance had already been exhausted. Some customers are embarrassed when told their card holds no balance and don't dispute the matter with the store or file a claim of fraud. Because customers tend to think of gift cards as "free money," they don't always take the same safeguards or file fraud or criminal complaints as they would if they were using credit cards.*

### **Web-Based Scams**

Some clever cyberthieves are taking advantage of gift card exchange websites such as CardCash.com and GiftCardRescue.com. These sites are popular because of the large number of gift cards that sit in sock drawers, unused, every year. About US\$3 billion in gift cards is expected to go unredeemed in 2020. [46] Customers can sell or exchange gift cards for a little less than the value of the card. Seeing an opportunity, scammers have used stolen credit cards to buy a bunch of prepaid gift cards and then flip them on the card exchange sites.

Although gift card exchange scams are pretty run-of-the-mill as far as theft goes, some internet scams are much bolder and more sophisticated. In recent years, scammers set up fraudulent Facebook pages with phony gift card giveaway offers. These pages used logos from well-known companies such as Best Buy, IKEA, Walmart, and Whole Foods to entice victims to become fans in order to win cards. However, the registration links on the pages usually directed users to affiliate marketing sites that collected personal data for marketing purposes. The scammers in a Whole Foods gift card promotion attempted to collect sensitive information for identity theft purposes.

With more than 2.50 billion active users worldwide [47], and because of its social networking focus, scams on Facebook can be highly successful—quickly. The IKEA scam lured more than 70,000 Facebook users before the pages were removed. In that case, the scammers created urgency—quite successfully—by stating “only available for one day.”

---

*Chapter 14 covers scams involving Facebook and other social networking sites in detail.*

---

Another way to draw victims to rogue web pages or sites is to use **typosquatting**. Scammers set up a fraudulent site, using a domain name that's just a character or two different from a legitimate social or company site. When a person accidentally mistypes the web address (domain name), he or she is directed to the fraudulent site, which looks very much like the intended site. The user is asked to complete a survey that gathers the person's name, address, phone number, and other personal information. Upon completion, the person is promised a free gift card. The person, now a victim, either never receives a card or receives a worthless card.

## Promotion Scams

Promotion scams come in many different flavors. A scammer may send a phishing email offering something very attractive—for example, free tickets on well-known airlines, free meals at popular chain restaurants, or a free smartphone or tablet. Getting this prize just requires clicking the link and registering. But of course, there's no prize—just harvesting of information.

Promotion scams are sometimes targeted to specific people in organizations, such as the president or CEO. In such cases, the lures include more upscale items, such as flights on private jets or complete vacation packages. The scams generally have the usual result—the victim either willingly enters sensitive information in a rogue website, or the victim's PC becomes infected with malware that harvests data in the background.

### ***“Improve Your Website Ranking!”***

*Another type of promotion scam targets organizations that recently set up websites. Soon after you proudly post your new site, your inbox is flooded with offers for website optimization, **search engine optimization (SEO)**, and search engine listings. Although you may have submitted your web address to some of the top search engines, you don't see your organization coming up in search hits, so the offers seem timely and attractive. The scammers know that search engines and directory submissions have lead times, and they're banking on your lack of knowledge of the process, or your impatience. You may pay the scammers to have your organization's URL listed in 50, 100, or more sites, but you get nothing.*

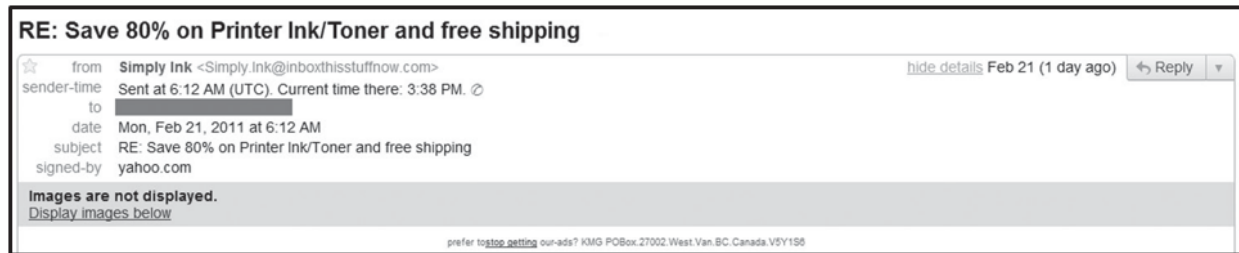
## Discount Scams

**Discount scams** work much like promotion scams: They offer products or services—in this case, at a discount—but usually don't deliver. One of the most prolific discount scams involves office supplies, cheating millions of dollars from organizations every year. In the pre-internet days, scammers routinely called small organizations and purchasing departments, selling bogus copier and printer toner, paper, and maintenance contracts. Now they send emails. Because consumables often wind up in the wastebasket or recycling bin, or hidden away in filing cabinets forever, companies are motivated to reduce those expenses. When an email arrives claiming to save you 85% on printer toner, for example, it's easy to fall for the trap.

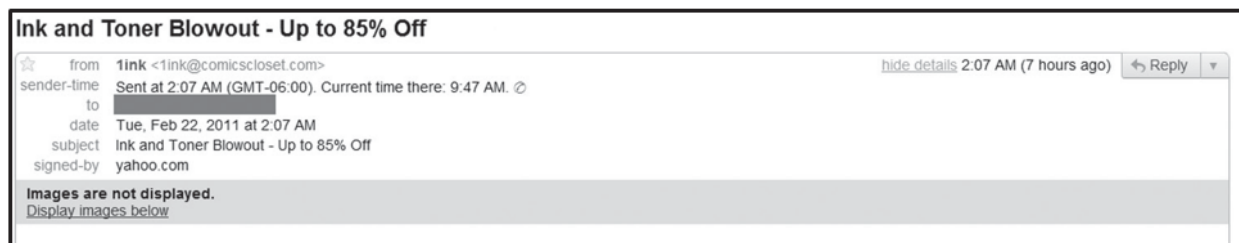
**Office supply scams** have a variety of purposes. Some are phishing emails, designed to gather personal information, usually for marketing purposes. You can spot these fairly easily because you'll often get two or more similar emails within 24 hours of each other (see Figure 37 and Figure 38). The first part of each email address looks like an office supply company. However, neither domain name comes up in an internet search, and neither domain name corresponds with a



supply company. The domain names shown in Figure 37 and Figure 38 were registered under the same address, but the company name and contact information were withheld.



**Figure 37** One email that offers discounted office supplies



**Figure 38** A second email offering discounted office supplies

In other cases, a scammer may accept your order and credit card payment but send nothing in return. Or the scammer might send your first order to you as you expect it. After that, the scammer may send inferior-quality products compared to those in the initial order, or it may increase the price substantially or send and bill you for mystery shipments that you didn't order. Some scammers simply begin sending regular invoices without sending any products, and they use bullying tactics to get you to pay those bogus invoices.

You may be able to use <https://www.whois.com/whois> to find out the owner information for the domain.

## Bogus Account Credit Scams

It's fairly easy for criminals to steal an organization's identity. A person or fraudulent company can usually garner enough information from yellow pages ads and an organization's website to pull off this kind of heist. At a very basic level, the criminal doesn't need much more than a prepaid cellphone and a box at a storefront postal center to go into "business."

Hiding behind the anonymity of the internet, such fictitious organizations are able to open credit accounts, buy goods and services, and shut down well before the first credit statement arrives.

## Chapter 13

### Retailer Scams

*These fraudulent companies and people, who only exist online, are known as **synthetic identities**. Some synthetic identities have such active financial histories that they end up having high credit scores and some financial institutions jokingly say they are hesitant to remove them when they discover them (even though they must by law) because the contact information can be resold for good money to other vendors and advertisers.*

According to the *CyberSource 2019 Online Fraud Report*, the most effective method of fraud management (in the “validation services” category) used by online merchants is the card verification number (CVN) from the back of a credit card followed by the order history check.

Financial websites such as PayPal contribute to the problem. As mentioned in Chapter 10, using PayPal is generally a safe way for consumers and organizations to make online payments, and millions use it regularly. However, almost anyone can open a PayPal account, and it takes little time if you have the required information. It’s also difficult for legitimate organizations to know if the company they’re dealing with via PayPal is legit.

PayPal requires some personal information, an email address, proof of identity, a telephone number, and bank account information. All of this is easy for a savvy scammer to provide. For example, a scammer can use a fictitious name and address, and set up a free email account on Hotmail, Yahoo, or Gmail. The telephone number can be a prepaid cellphone number or a VoIP account number, such as a Skype number. Many banks let you set up an account online by simply scanning your ID (which in this case will be fake). The scammer can verify his or her identity by acquiring a fake credit card, a virtual credit card, or a prepaid debit card. It may take some prep work, but the rewards can be great, and the bad guys have this down.

#### ***The Fake Receipt-Generator Scam***

*In 2010, scammers began targeting sellers on Amazon with fake receipts. Thieves downloaded a receipt-generator program from the internet that displays an input form very much like the form from any point-of-sale system. It even includes fields for details such as total before tax. The thief enters phony transaction data, and then the software creates a realistic Amazon receipt and “Printable Order Summary” page. The thieves then contact Amazon sellers, saying they have a problem with an order, and attach the receipt. A seller might not check his or her records, but may simply accept the receipt and send the scammer a partial or full reimbursement.*

## How to Avoid Retailer Scams

How can organizations defend against devious and sophisticated fraudsters? Education. The more you and your employees know about the individuals and companies wanting to do business with you, as well as the potential scams you could fall for, the better equipped you’ll be to

recognize and control fraud risk. Cybercriminals are global, and many are well organized and experienced. Learning their game plan helps level the playing field.

## **Gift Card Scam Protection**

Avoid buying gift cards from a store display rack; check with customer service instead to see if they have cards behind the counter. If you do purchase off the rack, carefully examine the packaging to look for signs of tampering. Look for a card that has a scratch-off coating on the back that conceals the card's personal identification number (PIN). If you can see a PIN number, grab a different card.

Watch as the salesclerk scans the gift card and hands it to you. Verify your receipt before leaving the checkout counter and keep the receipt as proof of purchase. If you purchase a card online, do so only from the store or company issuing the card. You might get a discount from another source, but why risk it?

*Comdata, a major processor of gift cards, recommends that retailers run exception reports regularly to uncover "prolific users." These are individuals or companies that make several calls per month or inquire on multiple cards from the same computer. Retailers can block access to those cards until any problems are clarified or resolved.*

## **Promotion and Discount Scam Protection**

As you know by now, it's important to think before you click. If a promotion or discount is out of the ordinary, it's probably a scam. To prevent discount office supply scams, route all purchasing through a designated employee. The employee should issue each supplier a purchase order (PO) with a PO number and manager's signature. This person should also inform the supplier that all shipments must include the PO number on the invoice and packing list, or the shipments will be refused.

## Chapter 13

### Retailer Scams

If you find yourself in the middle of a scam, don't pay the invoice and don't return any unordered supplies. Contact one of the following for assistance:

- ✓ Federal Trade Commission (<https://www.ftccomplaintassistant.gov>)
- ✓ Your state attorney general
- ✓ Your county or state consumer protection agency
- ✓ The Better Business Bureau

### ***Bogus Account Credit Protection***

As mentioned previously, running a credit history check is one of the best methods of authenticating a business-to-business (B2B) credit application. An organization should verify and validate all information on an application, including personal guarantors.

*It's best to check credit application information against several sources rather than rely on a single resource.*

\*\*\*

Consumers and businesses use their computers and smartphones to purchase vast numbers of products of the internet. The retailers get hit with fraud constantly. Thieves use techniques such as gift card scams, brick & mortar scams, promotion scams, discount scams, and bogus account scams in their quest to steal money and goods.

# Chapter 14

## Social Networking Scams

As you've learned in previous chapters, phishing takes place in a variety of ways. No matter what methods cybercriminals use, their primary goal is to entice you to click a hyperlink. Once you do, the site you visit may ask you for personal information, such as passwords or a social security number. By now, you know not to provide any information in response to a suspicious email.

But even if you don't provide information, just clicking the link and going to the site may quietly download malware onto your computer—a drive-by download in action. Then a keylogger records your keystrokes, and a Trojan program sends them off to the cybercriminals. Malicious hyperlinks can appear anywhere, even on the most popular social media websites.

*The most important way to protect yourself online is to follow KnowBe4.com's motto: "Think before you click." If you don't click, you don't open yourself up to potential danger and the many headaches that come with having your money and/or your identity stolen.*

This chapter takes a look at scams on social networking sites. While reading the chapter, it's important to understand the difference between the terms social networking and social media. These terms are sometimes used interchangeably, but they are not the same. One involves relationships, while the other is the tool used to create those relationships.

### *What Are Social Networking and Social Media?*

Networking of any sort involves relationships. Social networking involves being actively engaged in online conversations with other people or groups of people. Communication is multidirectional because social networking is all about connecting, collaborating, and sharing information freely.

Social media is the platforms, or channels, used for social networking. Just as radio and television are communication channels, Facebook, Twitter, blogs, and YouTube are communication channels as well. These sites are the tools used to share information, but they are not multidirectional communication. They simply provide the foundation for social networking to take place.

## *Watch for That Lure; It's Probably Obscured*

Many SMEs spend a lot of time and effort marketing their brands, products, and services on social networking sites like Facebook and Twitter. Today, these social media channels are valuable tools that any SME can use to reach its target audience. The social networking environment feels safe and friendly. Because of this, our guard is down when commenting, Tweeting, or instant messaging on these sites. This is especially true when the communication is associated with a known and trusted organization. Cybercriminals expect you to be relaxed and at ease on social networking sites. As a matter of fact, they're dependent on your guard being down in order for their scams to work.

However, the enticing ad, the email, or the direct message from a Twitter follower or Facebook friend are all you need to become a victim. The success of every phishing scheme depends on a few things:

- ✓ **Your lack of knowledge:** Fortunately for you, you're learning about the dangers lurking on social networking sites. Knowledge of the different types of fraudulent activities in cyberspace is one of your most powerful weapons against cybercriminals.
- ✓ **Your lack of attention:** Nobody's perfect. Even those of us who are knowledgeable about the ins and outs of cybercriminal behavior may accidentally click a link. Many times, these mistakes result from not being alert when clicking.

*A **follower** is a Twitter user who subscribes to another Twitter user's tweets. Followers see tweets from these subscriptions on their home page.*

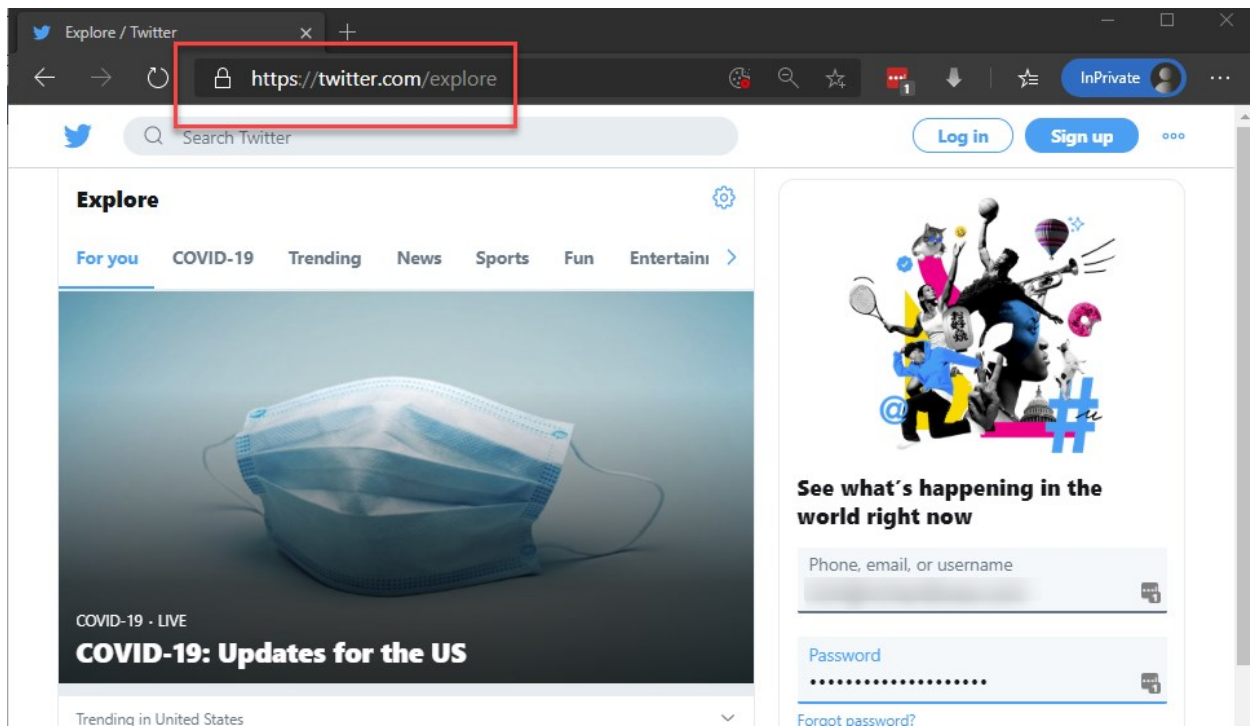
## *Anatomy of a Twitter Phish*

The initial goal of Twitter phishing scams is simply to get you to click. One popular Twitter phish example sends you an email notification that you have a Twitter direct message. The message may say "Hey, check out my blog post" or "lol, is this you?" and provide a link. The link directs you to a site that imitates the Twitter login page. If you click the link and enter your Twitter username and password, the cybercriminals have your login information.

With your information, the crooks send out direct messages under your name. These messages could trick your followers into also clicking the link because they believe they have received a message from you. Instead of going to a fake login page, your followers receive spam links that download malware to record every keystroke they make, including passwords and credit card information.

If you're directed to a Twitter login page, check the uniform resource locator (URL) in the address field of your web browser, as shown in Figure 39. If it has anything other than the twitter.com as

the domain name, do not sign in. If you do, you could be giving your username and password to cybercriminals.



**Figure 39** The real Twitter home page shows *twitter.com* in the address field of a web browser

If you click on a link within a tweet, you also put yourself at risk. Many legitimate tweeters use shortened links from sites such as bit.ly or tiny.cc because of Twitter's 280-character limit. Unfortunately, you don't know which links are legit or where they'll take you until you click them.

*If you're not sure about a shortened URL, use <https://www.expandurl.net/> to expand the link and see the full URL or follow one of the previous recommendations concerning how to expand shortened URLs. Your other option? Don't click on the short link.*

## Paying for Services You Don't Want or Need

Cybercriminals are experts at hiding or waxing over information to prevent you from knowing the truth. One example you'll find on Twitter is a service claiming to get you thousands of followers quickly. This is an appealing offer to an SME wanting to build a following quickly. The criminals say that they do this by identifying other Twitter users who auto follow anyone who follows them. They may also claim to have users segregated by interests or geographic location, so you can be sure your tweets are targeted to the right market. Even if you're charged for the

## Chapter 14

### Social Networking Scams

service and the efforts are successful, cybercriminals who get you followers this way are like spammers who sell email addresses. Be careful accepting such offers because you could be accused of sending Twitter spam and be banned from Twitter.

Another example is work-at-home advertisements that promise to help you make easy money. You use your credit card to sign up for a modest fee. Then you're charged a recurring monthly fee to receive additional tips, but the explanation of the amounts you pay is hidden or nonexistent. If you discover any charges, contact your credit card company within 60 days of the charge and put your request in writing in order to get your money back.

## *Anatomy of a Facebook Phish*

As Facebook becomes more and more popular, cybercriminals are finding new and better ways to use it to phish for potential victims. Facebook experienced the fourth largest number of phishing attacks in 2010, right after PayPal, eBay, and HSBC. Since that time, Facebook has gone to great lengths to reduce spam, phishing, and other scams, but even so, in the second quarter of 2015, Facebook had risen to the second highest site for phishing attacks, with Yahoo being the first [33]. Phishing attacks on Facebook are like attacks through email and other social media.

A common phishing scheme on Facebook involves a cybercriminal using your account to post updates with links on your friends' walls. When friends click such a link, they go to a fake Facebook login page. If they enter their email address and password, the cybercriminal can access their Facebook profiles and the personal information in their profiles.

In another scam, cybercrooks send fake emails with "Facebook" as the sender. The email says that your password has been reset and provides an attachment that supposedly contains your updated information. The attachment is actually a malware program. When you open the attachment, the malware installs on your PC. The software gathers not only your Facebook password, but all other passwords used on your computer.

The following sections describe additional Facebook scams to be aware of.

### **Quizzes and Other Applications**

On Facebook, you'll see **quizzes** like "What season are you?" or "Which Star Wars character do you resemble most?" Seems innocent enough, right? Wrong. Every time you accept a new application, you're giving a third-party developer access to your profile information. Sometimes these developers are fraudulent marketing companies trying to get you to buy services you don't need.

For example, Facebook experienced a scam advertising an IQ quiz. You click the ad and answer a few questions. Then, to receive your results, you enter your phone number. When you give your



number, you are unknowingly agreeing to additional charges on your phone bill each month. Cybercriminals don't display the terms of this fee, so charges can vary from small amounts to costs that can put a severe dent in your budget if not caught quickly.

## ***Instant Messaging***

Cybercriminals can get access to your Facebook profile through instant messaging. Once your account is stolen, the criminal can send chat messages to your friends, asking for money. Generally, the message says that you've been robbed and are stranded in another country, with no funds to get home. The message then asks your friend to wire money to you as quickly as possible.

## ***Spamming***

Some applications send notifications to all your friends and invite them to use the application because you're using it. The application then spams your friends, displaying unwanted advertising to those who signed up.

## ***Videos on Facebook***

You may receive a message with a link that appears to be from a friend, encouraging you to watch a video. Clicking the link takes you to a fake YouTube page where you're prompted to "upgrade your Flash player now." If you download the file, you download and install the Koobface (or other) worm. Your computer then automatically logs in and sends similar messages to your friends.

# ***Phishing and Other Social Media***

Phishing attackers like to target Facebook, but they're happy to share the love with other social media sites. Just as you should be suspicious of clicking any links on Facebook, you should also be suspicious of clicking any links for these other social media sites.

## ***YouTube***

SMEs, as well as large corporations, are turning to YouTube to make money or strengthen their brands through video sharing. The intent is to ultimately drive traffic to their own websites. Traffic-generator companies advertise on YouTube and via email that they will help you "earn subscribers," but they are usually fraudulent companies looking for victims. The thieves ask for your username and password, and often your credit card number. As is the case with most phishing schemes, you're at risk of identity theft, account theft, or malware infection.

## Chapter 14

### Social Networking Scams

Some scamsters take advantage of current disasters, such as the COVID-19 pandemic, earthquakes and tsunamis, the ongoing war against ISIS, or a major terrorist attack, by posting videos promising miracle stories from survivors. The video is supposedly hosted on a different site because of copyright issues. If you click the link, you may be presented with a survey you're required to complete to view the video. The survey is actually a phishing scam. Another version gets users to click link results in a pop-up window that states you must install a toolbar or some other software to view the video, but the program is malicious. A few years ago, a staggering three million YouTube pages were covered by an invisible Flash object/layer that took the user to a fake antivirus page. From that page, malware could download without the user's knowledge. The site came up when searching "Hot Video."

### ***LinkedIn***

Cybercriminals not only steal identities on Facebook and Twitter, but on LinkedIn as well. Most of us believe that LinkedIn is safer because it's more professional, but that's not the case. Cybercriminals create false profiles with pictures of models to get access to a variety of individuals throughout the site. The criminals often join group discussions, and then post comments with fake freelance job offers and links to their (rogue) websites. They also may simply "spam" discussions with marketing-related comments and links.

### ***Blogs***

Setting up fake blogs is a popular way to sell everything from office supplies to online training to subscription services. For example, a blog may follow an IT manager through a series of management training courses. The manager writes weekly about the materials and topics covered in the course and is open about his or her struggles and victories throughout. The manager also includes information about upcoming class dates and cities where training is offered, along with a website where readers can sign up and pay for the training.

While the charges are real, the training isn't. Neither is the IT manager. Scams like this are difficult to detect because you relate to the IT manager through the blog posts. Once you feel you "know" this person, it's much easier to hand over your credit card so you can attend the next class or training session. Advertisements for these types of blogs tend to appear on social networking communities that are IT-related, so be aware, do your homework, and use good judgment before you buy.

## *How to Avoid Phishing on Social Media*

The following are some general precautions you should take when using social media sites:

- ✓ Do not click on links in any email from a social networking site. If you think an email might be legitimate, ask the sender by phone or in person if he or she sent the email. If the link is for a website, go to the site directly by typing the address into your web browser.
- ✓ Beware of anyone asking for money through a social networking site. Cybercriminals might be able to get enough information to impersonate a coworker or an acquaintance.
- ✓ Do not download updates from an email link. Always go to the site directly through your web browser.
- ✓ Always check the URL before logging into any social networking site.
- ✓ Never re-enter your login information after you've already logged into the social networking site.
- ✓ Keep your security software up to date and make sure it runs continuously.
- ✓ Google your organization occasionally to see what kind of information you find about it on the internet. Cybercriminals can also find that information and use it to hack your social media and other accounts.
- ✓ If your account has been hacked, change your password immediately.
- ✓ Make your passwords stronger with special characters and change your passwords every few months.
- ✓ Pay attention when reading emails and when you're on social networking sites. Try not to read when you're tired and not alert enough to spot potential phishing or scam activities.
- ✓ Don't share sensitive information on any social networking site.
- ✓ If you freely accept every invitation to follow, friend, or connect, be careful about the information you share. Adjust your settings to let people see only what you want them to see.
- ✓ Be cautious of any shortened URLs like bit.ly or tiny.cc. If you receive a link from a colleague and believe it's legitimate, cut and paste the link into <https://www.expandurl.net/> to determine the actual target address.

## **Twitter Precautions**

Be extremely wary of short links that offer you coupons, prizes, gift cards, or work-at-home opportunities. Many free services, such as Twitpic, are designed to enhance your time spent on Twitter. However, don't assume that every service with "twitt" or "tweet" in its name is legitimate. If you're interested in using a free app or service, search for the name on the internet and read independent reviews first.

## **Facebook Precautions**

SMEs should regularly review the security of their company Facebook pages and any associated campaigns. Adjust your Business Page settings and permissions and be sure to continuously monitor the comments and discussions taking place on your Business Page wall. In addition,

## Chapter 14

### Social Networking Scams

listing your workplace or company affiliation on Facebook is fine as long as you protect yourself while you're at work. Edit your personal profile application and website settings on Facebook to limit access to your information. Here's how:

1. On the far top right of your Profile page, click the down arrow and scroll down to and click **Settings & Privacy**, then click **Settings**.
2. Under "Apps and Websites" you'll see a list a list of Active, Expired, and Removed applications.
3. Edit the appropriate settings to adjust who sees your information.

### ***LinkedIn Precautions***

Before accepting an invitation on LinkedIn, check out the person's profile. If it looks suspicious, click Ignore to refuse the invitation to connect. The same principle applies to group discussion links; to avoid a scam, check the profile of any group participant who offers potential work.

### ***Blog Precautions***

Here are a few ways to determine whether you're reading a fake blog:

- ✓ Do the photographs of the blogger seem too "slick"?
- ✓ Does it have fake endorsements by someone like Dr. Oz or Oprah?
- ✓ Does the offer for free items seem too good to be true?
- ✓ Is there a deadline for purchasing?

If you suspect you're reading a fake blog, don't buy anything on it or get tricked into running a program or clicking on a link. You could be handing your credit card information to a cybercriminal or unknowingly running a Trojan program.

\*\*\*

Using social media is an excellent way to stay in contact with friends, relatives, and acquaintances. Actively engaging and collaborating with other people and groups across the internet can be very fulfilling. However, you must be careful to protect yourself by using caution when clicking on links and common sense when reading posts.

# Chapter 15

## Ransomware

Ransomware is a type of malware that infects a computer or device and attempts to force a victim to pay a fee or ransom to regain access to files, prevent the revelation of private data, or keep something further malicious from happening. When it first appeared, this form of malware encrypted all the files on a computer and demanded a fee to restore access, but over the years, criminals have become more creative about their demands and the harm that they threaten to cause.

Since 2005, ransomware is one of the most significant threats to the cyber world. In fact, ransomware is now available to criminals in prepackaged forms complete with support hotlines so that virtually anyone can use or create their own variants to take advantage of this profitable form of cybercrime.

### *History of Ransomware*

Ransomware burst on the scene in 1989. A malicious Trojan targeted a healthcare mailing list and promised information and a quiz on AIDS (acquired immunodeficiency syndrome). The attack was delivered on 20,000 floppy disks and obscured names of files on the target computers. Victims were forced to pay US\$189 to recover their files. [51]

***Table 5 Some Notable Events in the History of Ransomware***

1989	First ransomware program was the AIDS Cop Trojan
2005	First contemporary ransomware programs began to show up, using asymmetric encryption
2013	CryptoLocker asks for bitcoin payment
2016	Samsam attacks using RDP brute force password guessing
2017	Petya attacks Ukraine
2017	NotPetya attacks Maersk causing US\$300M in damages
2017	Wannacry – Used 20 localized languages

From these early and somewhat unsophisticated beginnings, ransomware transformed into far more sophisticated and formidable types of attacks. For example, in 2006, the Archiveus Trojan

## Chapter 15

### Ransomware

encrypted everything in the My Documents folder, forcing victims to purchase something to decrypt their files.

The introduction of Bitcoin in 2008 gave cybercriminals an easier method to get paid without building in a payment engine and, for all practical purposes, in an untraceable way. A popular scheme at this time involved a fake antivirus program which tricked victims into paying money to fix problems that either didn't exist or were exaggerated.

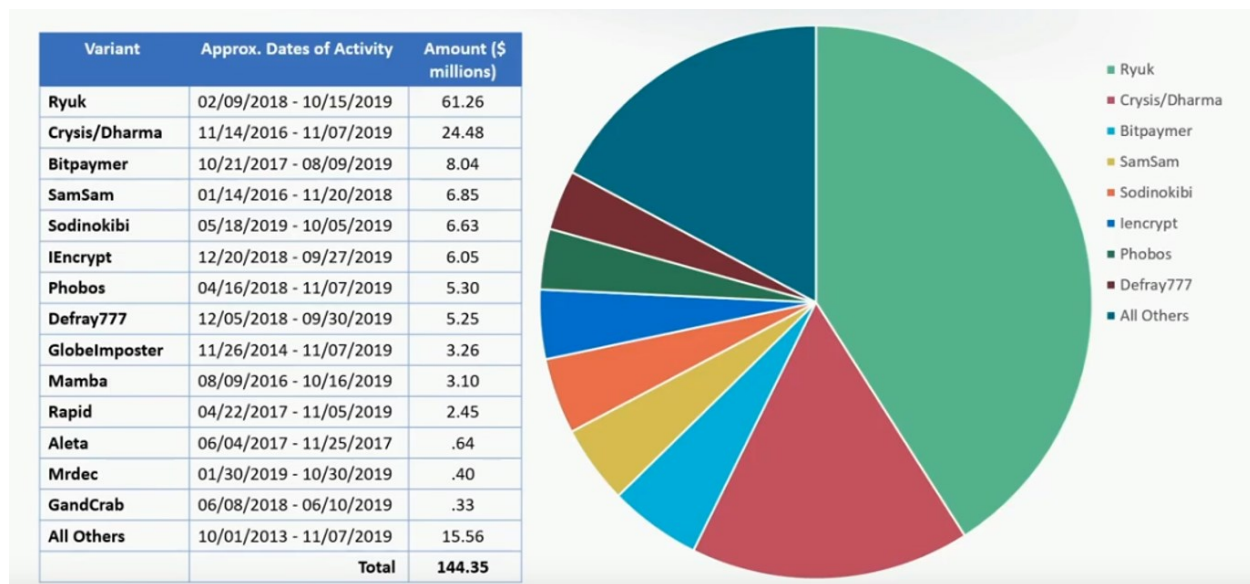
In 2011, a new ransomware variant appeared that installed a fake Windows product activation screen. Victims were required to call a number to get an activation code using an international premium phone call.

Another Trojan called Reveton followed in 2012 by locking victims out from their computers with a screen that made it appear that authorities had discovered the victim engaged in illegal activities. Payment of a "fine" was required to unlock the computer.

Attackers gained an estimated US\$27 million when they unleashed CryptoLocker in 2013. This malware demanded victims pay US\$400 and bitcoin within 72 hours or the encrypted files would be erased without recovery. This ransomware infected over half a million computers, the largest number up to that time. In 2015, the stakes grew even higher when CryptoWall v3 netted criminals an estimated US\$325 million. [52]

WannaCry appeared in 2017 and dwarfed the scale of previous attacks by penetrating over 200,000 victims in 150 countries. Many major organizations in the United Kingdom were completely debilitated and human lives could have been endangered. [53]

Figure 40 tracks just what the FBI knows about in ransomware payments between 2013 - 2019. The overall payments in the U.S. and elsewhere were many times higher.



*Figure 40 Which ransomware variants raised the most money?*

## Ransomware Basics

Over time, the focus of ransomware went from a consumer-focus asking for a fixed fee to a business-focus demanding a revenue adjusted ransom. Early forms used to encrypt immediately upon executing and didn't care where it was. Later, ransomware spread like a worm and then encrypted and encrypted as much of the victim's organization's computers and data as possible. Contemporary ransomware breaks in, dials "home" to notify the hacker or ransomware gang, who then figures out the best strategy and directs the malware to act accordingly. Actions taken can include any or all the following:

- Determines what to encrypt to make the victim cry uncle fastest
- Determines ability of victim to pay how much
- Disables/corrupts online/offline backups

Ransomware can exploit your system in several different ways. One common method is via phishing emails with attachments containing malware or links to malicious websites. These phishing messages use social engineering to trick victims into thinking the message is legitimate. Clicking on a link or opening an attachment downloads a malicious application, which will then install the ransomware onto the computer.

Another popular method is using a technique called malvertising, which stands for malicious advertising. Online advertisements can be infected with scripts and code. For unpatched systems, malvertising involves downloading and installing ransomware without user interaction; the

## Chapter 15

### Ransomware

victim only needs to view the advertisement to receive the malware. Otherwise, the malware will use social engineering to trick a user into downloading and running a file.

Virtually any other method can be used to distribute ransomware. For example, cheap USB flash drives can be infected with malicious code and then handed out for free at trade shows or even scattered on the ground for people to find. Once these flash drives are inserted into a computer, the code will either automatically run or be executed when someone clicks on a file. Running the application on the USB key installs the ransomware on the computer.

There are several types of ransomware, including the following:

- **Scareware.** This type of malware attempts to scare the victim into paying a fine, purchasing unneeded technical support or installing unnecessary or useless security software. In one variant, pop-ups appear periodically to suggest that your computer needs repair or assistance. These pop-ups are annoying and will continue to appear until a fee is paid or the malware is removed. Another contains a message with a fake law enforcement warning saying they have caught the victim doing something bad or that the user was filmed watching porn.
- **Screen lockers.** These lock victims out of their computers and demand payment to restore access. They often attempt to scare people into paying by claiming the victim has committed some sort of illegal activity.
- **Encrypting.** In this type of attack, the files on the victim's computers are encrypted and then payment is demanded to restore access.

Traditional ransomware is getting more sophisticated. It remains in the victim's environment much longer to do analysis and research. Ransomware gangs use built-in, trusted tools, such as PowerShell, and maliciously encrypt VMs or data backups with their own encryption keys. You may believe you have great backups when you really don't.

Some variants are available as **Ransomware-as-a-Service (RaaS)**. The advantages to the criminal include: the malware is constantly updated all the time, avoids antivirus detection, and is controllable from a central console by the hacker.

Victims are paying more often for several reasons, mostly because the ransomware is successfully encrypting more data, deleting backups, and forcing the victims to pay to get back up and running. The use of cybersecurity insurance companies have also led to more paying of the ransomware because insurance companies want to pay less overall, and paying the ransom is usually less costly than not. A typical scenario for someone with cybersecurity insurance looks like this:

- The victim calls the insurance company.
- The insurance company calls an incident response broker who specializes in ransomware attacks.



- The broker calls all the needed specialists and has all the needed relationships.
- The broker hires and/or directs the “stop-the-damage” specialists.
- The broker hires the recovery specialists.
- Professional, full-time negotiators handle the ransom payment (amount to pay, etc.).
- Media response teams handle any public relations issues.

## *Traditional Ransomware*

Some forms of malware take over a computer, encrypt all the files, demanding that anywhere from hundreds to millions of dollars be paid to decrypt everything. The victim is forced to pay the ransom if they want their files returned to a usable state. Some ransomware locks users out of their systems without encrypting files.

## Chapter 15

### Ransomware

Example ransomware screens are shown in Figure 41 and Figure 42 below.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.  
**How to buy CryptoWall decrypter?**



- 1. You should register Bitcon wallet ([click here for more information with pictures](#))**
- 2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**  
*Here are our recommendations:*
  - [Coin.mx](#) - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
  - [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly.
  - [bitquick.co](#) - Buy Bitcoins Instantly for Cash
  - [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
  - [Cash Into Coins](#) - Btcoin for cash.
  - [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
  - [anxpro.com](#)
  - [bittylicious.com](#)
  - [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
- 3. Send 1.19 BTC to Bitcoin address: [16ydt1Wj2NZa2uLZ6W4UDCDJ2Ttw92uFaT7](#) [Get QR code](#)**
- 4. Enter the Transaction ID and select amount:**  
  

[Clear](#)

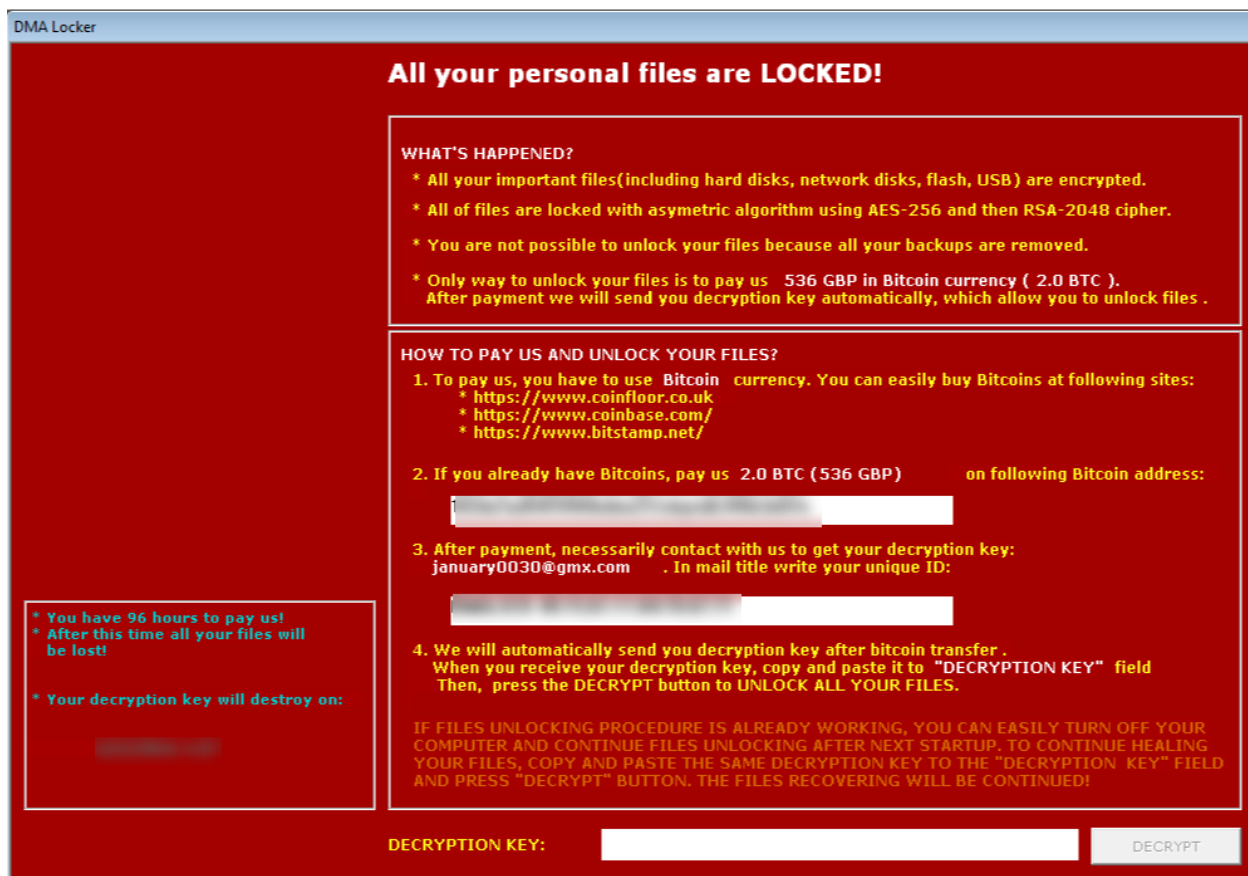
**Note:** Transaction ID - you can find in detailed info about transaction you made.  
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)
- 5. Please check the payment information and click "PAY".**

[PAY](#)

Your sent drafts				
Num	Draft type	Draft number or transaction ID	Amount	Status
Your payments not found.				

**0** valid drafts are put, the total amount of **0** USD/EUR. The residue is **500** USD/EUR.

*Figure 41 Example ransomware message*



*Figure 42 Example ransomware message*

Although ransomware is criminal extortion, your computer is infected using exactly the same methods as other malware, including drive-by-downloads, opening infected attachments, or clicking on malicious banner advertisements.

Ransomware may do one or more of the following actions on your computer:

- ✓ Encrypt one or more systems or data files.
- ✓ Spread to more computers.
- ✓ Allow ransomware hackers access to the environment so they can determine which assets to encrypt to cause the most operational and financial pain.

Depending on the type of ransomware infection, it can be very difficult to remove from your computers and network. Often, the encrypted files are unrecoverable, and you will have to reinstall the operating system unless you pay the ransom or can restore from a backup.

## *Ransomware 2.0*

Traditionally, ransomware only encrypted data and systems to cause operational issues and downtime. Starting near the end of 2019, cybercriminals started using ransomware to add more maliciousness to ensure that they get paid. They realized that with the access they had to the exploited systems and networks, encrypting data and systems was the least of what they could do. Encryption could be defeated by a good backup and the ransomware gangs were tired of not getting paid by people with good backups.

As a result, this is what many ransomware programs (some call it Ransomware 2.0) do now:

- ✓ Encrypt data and files of every system they have determined is critical to the victim.
- ✓ Steal network login credentials.
- ✓ Steal customer credentials, if available.
- ✓ Steal employee personal and work credentials.
- ✓ Exfiltrate data and credentials.
- ✓ Request a ransom to decrypt files and not to release data and credentials to the public or malicious hackers.
- ✓ Publicly reveal that the victim company has been successfully attacked and what data and credentials have been stolen.

By encrypting AND stealing data and credentials, hackers still have extortion leverage over the victim even if the victim has a good backup. Each victim must now weigh the costs of not paying a ransom and seeing their data on the web where it can be abused by hackers and used to their competitors' advantage. Most companies have critical secrets, intellectual property, and private communications they would rather their customers and the world not know. Using this new strategy, ransomware gangs are getting paid more now than ever.

## *More Malicious Ransomware*

As of the end of 2019, ransomware is becoming even more malicious and the types of attacks more varied. Ransomware crooks wanted to increase the rate of victims paying the ransom. It didn't take them long to realize that their main asset was the admin access they had to the victim's computer systems and networks. Because of this, encrypting the data and holding it hostage has become the least of the victim's worries. A few of the specialized attacks are described in the following sections.

**Steal or Leak Data.** Hackers often begin by determining the company's "crown jewels" and then, based on what they found, copy gigabytes to terabytes of organization, employee, and customer data. The hackers can then threaten to publicly post trade secrets and other information or give it to the victim's competitors.

For example, in 2019, Allied Universal, a U.S. security company, was hit by ransomware. The computer data was encrypted, and the hackers obtained access to many sensitive files. The ransom of US\$2.3 million wasn't paid, which resulted in 700 MB worth of stolen data being published. [54]

In retaliation for not paying the ransom, a ransomware gang pilfered and published data from Boeing, Lockheed Martin, and SpaceX. These documents included sensitive military equipment, billing and payment forms, legal paperwork, and outlines of SpaceX's manufacturing partner program. [55]

**Auction Your Data.** If the hackers can gain access to confidential information, they may threaten to auction the data to the highest bidder unless the ransom is paid. For example, on June 2, 2020, Brian Krebs reported "Over the past 24 hours, the crooks responsible for spreading the ransom malware 'REvil' (a.k.a. 'Sodin' and 'Sodinokibi') used their Dark Web 'Happy Blog' to announce its first ever stolen data auction, allegedly selling files taken from a Canadian agricultural production company that REvil says has so far declined its extortion demands". Their auction page set the initial deposit at \$5,000 and a starting bid at \$50,000 to get three databases. [53]

**Steal Credentials.** Ransomware hackers focus much of their attention on searching for every credential they can find so they can steal them and reuse them to maximize pressure, future pain, and future financial gain. These gangs now extract every found organization, employee, and customer credential they can before revealing themselves and asking for ransom.

**Threaten Victim's Employees.** The employees of the victim can be targeted by ransomware hackers. They notify employees that they have their login credentials, Social Security numbers, and other personal information, and will threaten to release it to hackers or publicly on the internet if the overall ransom is not paid by the organization.

**Threaten Victim's Customers.** Customers of the victim may also be targeted. In this case, the criminals let the victim's customers know they have their logins and private data and will release it publicly unless a ransom is paid. They may also extort these customers directly.

Ransomware now targets MSSP (Managed Security Service Providers) and their customers directly. They compromise MSSPs and then compromise all their customers at the same time, hitting each customer individually or they tell the MSSP they have done so and demand payment or they will attack all the customer's computer assets and let the customers know they only did it because their MSSP didn't care enough about them to pay the ransom.

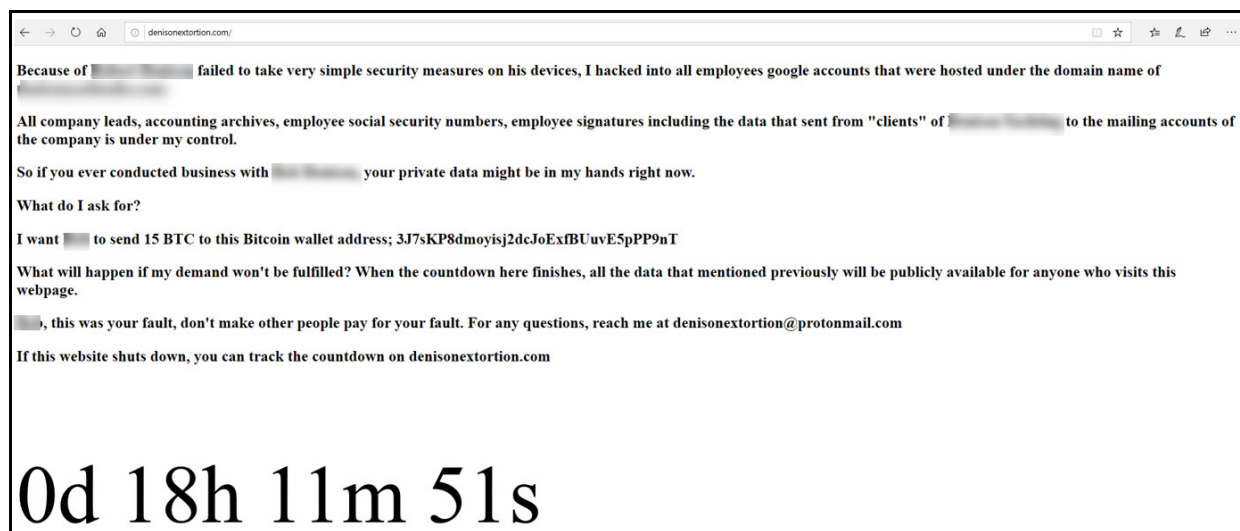
**Use Stolen Data to Spear Phish Partners and Customers.** Ransomware gangs also look through stolen data to find information that can be used against your business partners and customers. This is one of the fastest growing phishing segments.

## Chapter 15

### Ransomware

**Public Shaming.** Ransomware hackers will publicly reveal the victims of their ransomware programs, along with what was stolen (i.e. confidential data and logon credentials) so they cannot hide the exploitation from their customers or regulators.

**Threaten Everyone Involved.** To put pressure on the victim to pay up, ransomware criminals may resort to threatening everyone: customers, vendors, employees, stockholders, and anyone else they can think of. The hackers send out a message to these groups of people that confidential data may be released to the public with the idea that this will force the victim to pay up. Figure 54 shows a real-world example.



*Figure 43 Real World Example of Threatening Everyone*

## The Future of Ransomware

This is the new normal of ransomware on the internet. Ransomware is here to stay and is evolving rapidly because it's very lucrative financially and simple to implement. Criminals have a large variety of tools available to help them create new and more powerful ransomware attacks and they won't hesitate to make use of them. As long as it pays and attackers cannot be caught or arrested, it will stay around.

## Defenses

It's important to communicate to management (who needs to understand the risks) and users about how ransomware is changing. In the past, it was possible to depend on backups and other

measures to save you, but that's no longer true. Take the following steps to use as part of your security awareness training.

## ***Recognize the Problem***

Ransomware is not the real problem. The real problem is how systems become infected and administered. The list below shows the most common ways.

- Phishing
- Unpatched software
- Password guessing
- Misconfiguration

To stop ransomware, you must stop hackers and malware from breaking in and exploiting your environment. If you don't, you are never going to stop the ransomware from infecting your systems, stealing your data, blackmailing you and your users, and doing other nefarious acts. If malicious applications such as ransomware can get into your systems, they will always be able to do bad things.

The three top defenses include focusing on:

- Preventing phishing by using a combination of policies, technical defenses, and security awareness training.
- Better patching of internet-facing applications in a timely manner.
- Reducing the number of elevated accounts and using MFA where possible.

## ***Preventive Controls***

These are the best defenses against ransomware:

- Regular, defense-in-depth, computer defenses.
- Total, tested restores of backup of critical systems.
- Practice elevated credential protection/hygiene/monitoring.
- After a successful ransomware exploitation, change all possibly compromised passwords (e.g., software, employee, customer, etc.) and not just email or network login passwords.
- Get cybersecurity insurance.
- Discuss with management, incident response, and a media response team how to handle it if your organization gets hit by ransomware.

## ***Early Warning Detection***

Additionally, you must have early warning detection as described below:

## Chapter 15

### Ransomware

- You must detect the intrusion.
- Install tools (IDS, HIDS, NIDS) to make security personnel aware of packets being received by and sent from the network.
- Install Endpoint Detection tools on servers, workstations, tablets, etc.
- Use Crowdstrike-like monitoring client tools to detect threats in your environment.
- Install tools which have the ability to detect a massive number of suddenly changing files.
- Install Data Leak Prevention tools.
- Regularly perform a Network Traffic analysis.
- Monitor outgoing flows: computer-to-computer, server-to-client, client-to-client, server-to-server.
- Use honeypots to help detect and deflect attacks from production targets.

## **Communications**

Communications are vital. You need to talk to senior management, IT, communication specialists, etc., before breaches occur and work with them to put in place a plan.

Answer the following questions in your plan:

- Do you have a well-tested backup of all your critical systems?
- Decide ahead of time whether the organization will or won't pay the ransom.
- Are you ever paying the ransom, and if so, does management know what that means, including data loss, employee and credential theft, etc.?
- How and what do you say to employees and customers when their data, credentials and other private information is out there on the web?
- If you don't pay the ransom, how will your organization handle confidential data and sensitive emails (ex. disparaging customers and partners) getting out?

\*\*\*

Unfortunately, ransomware is here to stay. You can't bury your head in the sand and hope that it doesn't affect you and your organization. If you don't take proactive steps to be ready in advance, you'll find yourself scrambling for a solution and may wind up losing data or paying a ransom. No one wants to pay extortion money to criminals, so don't leave yourself in that position.

Chapter 23 goes into more detail about how to foster security awareness and the ways that KnowBe4 can help.



# Chapter 16

## Mobile Threats

Today, virtually everyone owns one or more mobile devices. You might have a smart phone in your back pocket, a Kindle in your suitcase for use on the airplane, and an iPad that you use while drinking coffee in the café. Each of these devices is a powerful computer complete with large amounts of storage, connections to the internet, and applications that can perform a variety of tasks.

To remain safe, you must take a few simple precautions to secure all your mobile devices. At the very least, protect your device by a login of some kind. This will at least prevent unauthorized access to your personal and private information. The remainder of this section goes over a few threats to your mobile devices and some suggestions about how you can mitigate them.

### *Lack of Login*

Think for a minute about what's on your smart phone or tablet. If you're like most people, you install applications for electronic banking, charge things to your credit cards, post on Facebook and other social media, and perform dozens or even hundreds of tasks for you throughout the day. Applications seem to be too useful to ignore. On top of that, your phone keeps a record of every phone call you've made and all the text messages you've sent or received. You've probably taken many photos and created some videos, and perhaps some of them were intimate and not meant for public disclosure.

Now consider that you carry around all this personal information in the palm of your hand or your back pocket. If that phone was stolen or misplaced, a malicious individual could access your financial data and learn many of your most personal secrets. With just your mobile phone, it wouldn't be hard for a malicious individual to drain your bank account, charge up your credit cards, and send all your photos and videos to friends and strangers on social media.

Wouldn't it be convenient if there was a way to protect your information from a casual thief? You think that they would build some kind of lock or combination into smart phones, wouldn't you? As it turns out, virtually every smart phone, tablet, and other mobile device includes the ability to lock the device so that only you can access the information on it. Some devices use a PIN, others require a fingerprint, and some even allow for even more sophisticated security locks such as facial recognition.

## Chapter 16

### Mobile Threats

The biggest threat to your mobile device is you. Leaving the device unlocked is the same as not locking your front door when you leave the house – you’re just inviting criminals to come inside and take whatever they want.

## *Malicious Public Hotspots*

Today it seems that every café, restaurant, hotel, and airport provide free internet access. Many of these access points don’t require passwords or usernames. Anyone can just connect at any time. You can access your bank, your social media, and everything else from virtually anywhere you happen to be.

Unfortunately, public access points are often not what they seem. Even though the name of that access point is “coffee shop”, that doesn’t mean that it has anything to do with a coffee shop. It’s easy for a hacker to set up a wireless router in a van next to the coffee shop and give it the name “coffee shop”. If you connect to the hacker’s Wi-Fi router, they’ll be able to see which sites you visit. Encryption can be helpful to minimize the risk, but even so, your information is still being routed through a hacker’s access point. Your connections could be affected by a man-in-the-middle attack (see page 225) and you might be sent or interact with a fraudulent website. Do you really want to take the chance? After all, they might have the tools needed to decrypt your data or otherwise cause you harm.

Be cautious about using public access points for anything personal, financial, or confidential. Make sure your connections are protected by HTTPS/TLS (i.e., the lock icon is present on the browser) AND that you are connected to the correct, legitimate URL. You must do both because rogue websites often have HTTPS/TLS enabled. Or, second, use a trusted VPN connection for all internet connections.

## *Malicious Applications*

There are literally hundreds of thousands of applications available for your Android or iPhone mobile device. These applications install on your smart phone and ask for the security access that they require to get their job done – and sometimes a lot more than they need. Many of these applications are granted the ability to read your contact list, turn on your camera, make phone calls, and perform any number of other tasks. Many mobile applications have been found to eavesdrop on or copy a user’s confidential information with or without the user’s permission or understanding.

While major organizations such as Google and Apple do attempt to verify these applications to ensure they meet security standards, it’s not uncommon for hackers to slip one through occasionally. On top of that, each application, even if it’s 100% credible, can contain security

vulnerabilities. They are, after all, written by human beings, often under extreme pressure to meet deadlines.

Follow these guidelines when considering whether you should install an application:

- ✓ Is the application really something that you need?
- ✓ Where is the application from – a single, a small company, or a major corporation?
- ✓ What privileges does the application require?
- ✓ Are you comfortable giving out access to the application?

Keep the number of applications to a minimum. As a general rule, if you're not using an application, uninstall it. Always review the permissions that an application is requesting and ask yourself if the requested permissions make sense. Are they worth the risk of assigning them to that application? When in doubt, don't install the application.

Never "jailbreak" your mobile device or install an application that requires jailbreaking. **Jailbreaking** means you are intentionally disabling many of the security protections of the mobile device that the vendor had enabled by default to protect you. Once a device is jailbroken, a rogue application can commit cybercrime against you and your device. A legitimate application never requires jailbreaking your device.

A rogue or poorly written application can allow malware to be installed or can give control of your mobile device to a hacker. Use caution about what you allow to be installed onto your device.

## *Phishing*

Many users of mobile devices monitor their email, social media, and text messages in real time. They open and read emails as soon as they are received, check their social media regularly, and respond immediately to text messages without thinking.

Because of this, mobile users are highly vulnerable to phishing and scams. Many times, emails and text messages only display the sender's name and a few obscure words or perhaps a sentence. It's tempting to just respond or click the link, but this can result in the installation of malware onto your mobile device. From there, the hacker can gain control and do anything desired from monitoring your keystrokes to adding your smartphone to a botnet.

Be cautious about clicking links within any email or other messages that you receive on your smart phone or mobile device. Don't respond to text messages unless you know the sender. Remember, if you give a hacker control of your phone because you clicked on a phishing link, you may have just given them access to all of your personal photos and videos, your banking information, and other private information.

## *Spyware*

Spyware exists for mobile devices in much the same way as it does on desktop computers and laptops. Generally, **spyware** is malware that sends data back to cybercriminals about your purchases, browsing habits, and even your GPS data. These can be installed along with applications, downloaded from websites, and received as attachments to emails.

**Stalkerware** is another threat that exists primarily on mobile devices. It consists of spyware that is installed by employers, coworkers, spouses, friends and so forth without your consent or knowledge. The purpose is to track your usage and whereabouts for their own purposes. A spouse, for example, might install a specialized program to allow them to track their significant other to see if they're having an affair or if they're spending money on things they shouldn't be.

Stalkerware is often installed directly on the device by an individual, but can also be installed remotely in some instances. These individuals may have access, making it easy to plant the malicious spyware applications. To prevent this, keep your mobile device locked and don't share the password or PIN number with anyone. Don't use work devices for personal uses. Instead, use your own personal smart phone or device. It's completely legal for your employer to install whatever they want on your phone and snoop into what you're doing if that phone is owned by them.

## *Data Leakage*

Mobile applications are notorious for unintentional data leakage. Your information could be inadvertently shared with people or organizations that are not authorized or are unknown to you. A prime example is free applications that perform exactly as specified, but also send personal information to an advertiser's server. Due to poor security, this information could also be intercepted or mined by cybercriminals.

Poorly written applications can also leak data over wireless, Bluetooth, or from the database or website of the application designer. To avoid this kind of problem, or to at least reduce the opportunities, only grant permissions that are absolutely required for the application to perform its functions. Don't install applications that demand more privileges than needed.

## *Lost Phone or Device*

A lost or stolen smart phone or other mobile device can be a disaster. It's amazing that such a tiny device can hold so much information that is personal and confidential. Think of how disastrous it would be for criminals to gain access to your bank accounts, credit card information, personal photos and videos, and passwords. Most people store all this information and more on

a device which fits in their back pocket and is easily misplaced. It's worse when you consider that many people don't even bother to secure them in any way, not even by using a PIN number.

Take the time to investigate the "locate my phone" function of your smart phone. Many modern phones include an application that lets you locate it from a remote location. Additionally, these applications may let you erase the data on the phone as well. Make sure your phone includes one of these applications and that you know how to use it. This should be one of the first things that you investigate after you acquire your new phone. This way, if your phone is lost or stolen, you can either find it or erase the private data from the comfort of your home. You may not retrieve your phone, but at least you won't be handing the cybercriminals the keys to your life.

## *Keep Your Mobile Device Updated*

Regularly update the operating system and applications on your mobile device. As with desktop and other computers, vendors are constantly at work patching their applications as they discover vulnerabilities. You can check for updates in the App Store on iOS in the play store on Android. This is very important, as new vulnerabilities are regularly discovered and patches are required to prevent criminals from accessing your mobile device.

\*\*\*

These are just a few of the vulnerabilities and threats to mobile devices. Remember that your smart phone, tablet, Kindle, or whatever other mobile devices you own are actually powerful computers. They often contain immense amounts of personal information that would be embarrassing or disastrous if released to the public or accessed by cybercriminals.

Take the time to understand how to secure your mobile device as soon as possible after purchasing it. With a few simple steps such as adding a PIN number and avoiding public access points, you can keep your information secure and private. If you don't take these simple steps, criminals could post your embarrassing information to the internet, drain your bank accounts, max out your credit cards, or even ruin your life.



# Chapter 17

## Nation State Threats

These days, it's not uncommon for the news to report about a cyberattack. Many of these are sponsored by criminal gangs. Other attacks originate from nation states such as North Korea, Russia, Iran, and China. The ubiquitous nature of the internet has created an easy way for countries to perform powerful attacks while remaining anonymous. Even when the nation states are identified, they can shift the blame to independent cyber gangs or individuals who have "nothing to do with them".

Cyberwarfare is the action of nations to attack the infrastructure, military, and businesses within other nations. These attacks can cause significant damage. For example, in theory, a cyber attack could cause a nuclear power plant to meltdown, a factory to explode, a power grid to fail, and airplanes to crash. In the military arena alone, cyberwarfare can cause havoc in the battlefield by taking control of drones, misleading air defense systems, and fooling radar and other equipment into thinking that attacks are not occurring or are happening in other places.

There are many ways that cyberwar can be used against a nation. These kinds of attacks can, of course, support military operations. In addition, they can provide immense amounts of information on the activities of militaries, governments, businesses, and individuals of other nations – in other words, spying. Nations can also use cyber propaganda to influence public opinion by using social media, fake news, and other methods to destabilize populations, influence elections, and manipulate governmental decision-making processes.

### *The Role of the Nation State*

A nation state is a legitimate sovereign entity ruled by a government. A nation state generally exercises its authority over the people living in a well-defined area of land with recognized borders, a military, and its own identity. There are exceptions in that some nation states are not recognized by others – for example, the Kurds occupy land within several nations and are not recognized by any government as an independent country. However, to a large extent, they have their own local government, identity, social support systems, and even a military in the form of militias.

All nation states are responsible for their own defense and offense, and the same is true of cyberwarfare. Networks and infrastructure must be protected. In the physical world, that protection consists of security guards, defensive missile systems, and air forces. Over the

## Chapter 17

### Nation State Threats

internet, infrastructure is defended with firewalls, anti-malware software, and teams of security experts.

Nations tend to focus most of their budgets and resources on offensive attacks. For example, the NSA – the U.S. agency responsible for monitoring and decoding communications outside U.S. borders – spends the vast majority of its cyber operations budget on cyber weapons designed to monitor, attack and destroy the infrastructure, communications, command-and-control, and other vital systems of hostile countries. A much smaller portion of its budget is dedicated to protecting the United States from other nation state attacks.

Nation states hire people or groups to disrupt, destroy, or compromise other governments, corporations, and individuals. Sometimes their mission is to gain access to secrets or other valuable information and other times, their role is to damage industries, militaries, and politics. Generally, nation states do their jobs covertly and virtually never acknowledge what they have accomplished.

In this way, they operate in a manner like spies and often take pains to cover their tracks to make it difficult for them to be traced, especially to the originating country. They may use social engineering techniques such as spear phishing or other actions to convince an unsuspecting individual to do something for them. They may also create fake profiles on social media platforms such as Facebook or embed themselves in an organization's supply chain.

Attacks from nation states can be particularly destructive because the hackers have access to the resources of a country, which can be significant. The people involved may also be strongly motivated by nationalism and feel they are part of a war against an enemy. This can make them far more dangerous than mere criminals. [57]

## *Zero-Day Vulnerabilities*

Attacks by nation states can use so called **zero-day vulnerabilities**, which are generally flaws in applications or operating systems that are not known to the vendor. Because they are not yet been widely publicly known, they are not patched, and the underlying software is vulnerable. It's likely that nation states maintain hundreds and possibly thousands of these zero-day flaws ready to use if needed. They are used sparingly because once the flaws have been exploited, they are more likely to become known by the vendor and patched.

Zero-day vulnerabilities are highly treasured by nation states – and cyber criminals as well – because it gives them the ability to break into computer systems and infrastructure more easily. As a result, the cyber warfare groups within nation states constantly research to discover these vulnerabilities. There is some debate about whether these vulnerabilities should be shared with their own country's cyber defenders so that defenses – patches – can be created. However, for the most part, these vulnerabilities remain secret, so they may be exploited when needed. The



result is that everyone – businesses, militaries, individuals, and organizations – throughout the world remains vulnerable and more at risk of being attacked.

## *Legalities*

There are significant difficulties in defining and enforcing laws against cyberwarfare. The UN Convention on Cybercrime, which went into force in 2004, is the first international treaty that sought to address cybercrime. Its goal was to increase the cooperation regarding cybercrime among nations. This convention was supported by many countries in Europe as well as the U.S., but is opposed by Russia, Brazil, and India, among others. Many nations believe a treaty such as this violates their national sovereignty.

Regardless, the UN Convention on Cybercrime does not define or address cyberwarfare, instead focusing on crimes such as illegal access, interception, interfering with data, breaking into systems, misusing devices, forgery, fraud, child pornography, copyright, and so forth. [58] This means that cyberwarfare is largely unregulated, and any enforcement is difficult, if not impossible.

In 2013, several major nations harmonized national laws regarding cybercrime. The law of state responsibility affirms that a nation (a state) is responsible for the actions of individuals who are under its “effective control”. The international Court of Justice decided that private individuals who violate international law are only the responsibility of a nation only if it can be proven that the state directed or controlled the action. It is the responsibility of a cyber victim to prove that a nation had “effective control” over every aspect of the attack. Without this proof, the only legal response for the victims would be against the group or people who performed the attack but not the nation itself. [59]

## *Military Uses for Cyberwarfare*

Today, militaries all over the world depend on the internet, satellites, and sophisticated technologies to improve and enable their war-fighting capabilities. For example, drones, aircraft, and ships depend on GPS signals for navigational and targeting. Interfering or blocking GPS communications are a major target for cyberwarfare, since doing so can effectively render dependent systems useless or severely degraded.

A few incidents of cyberwarfare are described below: [60]

- ✓ In 1998, the U.S. hacked into Serbian air defense systems. These were so effective that the U.S. feared it would damage civilian targets, causing it to cease the operation.
- ✓ In 2007, several terabytes of information was stolen by an unknown foreign entity who hacked into many high tech and military agencies of the U.S.

## Chapter 17

### Nation State Threats

- ✓ In 2008, a USB flash drive spread malicious code on classified and unclassified systems at the Pentagon. This is considered the most significant breach of U.S. military computers in history.
- ✓ In December 2009 through January 2010, a cyber attack was launched from China against over 20 companies, including Google.
- ✓ Beginning in 2012, the New York Stock Exchange and several banks suffered from a series of denial of service attacks. Responsibility was claimed by a hacktivist group called Qassam Cyber Fighters.
- ✓ In 2013, the U.S. Department of Defense stated that the U.S. would consider using nuclear weapons to respond to a cyber attack.

Cyberwarfare is now a critical component of militaries of virtually every nation. Every future conflict is likely to include its own cyberwarfare component to increase the military odds of success.

## Snowden

In 2013, a newspaper known as *The Guardian* published a story that claimed that the NSA was spying on American citizens. The story was based on top-secret documents and didn't mention that these were leaked by a single individual who, three days after the publication of the article, came forward and revealed himself as Edward Snowden.

The revelations leaked by Snowden revealed the immense significance and scope of the programs being run by the NSA against American citizens. The leaked documents showed that virtually every phone company in America was giving the NSA access to all their customer records. This revelation alone produced a huge uproar which led to reforms ordered by the House of Representatives and President Obama.

A program called PRISM gave the NSA the ability to request user data from companies such as Google, Apple, Facebook, Microsoft, and others. These businesses are required by law to hand over the information upon request. The U.S., working in concert with the British government communications headquarters, tapped fiber cables throughout the world with the goal of being able to snoop on global internet data. This program is code-named Tempora and gives the British and American governments access to virtually all information flowing through the fiber-optic cables that are strung under the oceans and between countries.

The NSA created a tool called Xkeyscore, which allows it to find out virtually everything done by anyone on the internet. To facilitate their ability to read the information flowing through fiber-optic cables and other infrastructure, the NSA has worked to force companies to weaken their encryption algorithms or install backdoors. They have also hacked into servers and computers.

On top of that, the NSA intercepts hundreds of millions of text messages daily in a program called Dishfire. They can also intercept and decrypt cell phone calls and encrypted text messages. There are many other programs, some known and some which remain secret, run by the NSA intended to gather intelligence about anyone or anything on the planet and attack countries, businesses, or individuals as needed.

## *North Korea Sony Pictures Attack*

In 2014, North Korea was incensed by a film produced by Sony called “The Interview”. This was a comedy about a plot to assassinate the North Korean leader. A group known as the “Guardians of Peace” leaked confidential data from Sony pictures that included personal information about Sony employees and their families. The leaks included emails about clients that showed that senior executives were sometimes very dismissive and insulting of several big stars. The hacker group then used a variant of the Shamoon Wiper malware to erase the computer infrastructure of Sony pictures.

The attack was successful in getting Sony to cancel the formal release after many United States cinema chains decided they would not show the film. Instead, Sony distributed the film in a downloadable digital release. The United States government claimed the attack was sponsored by the North Korean government, but the North Koreans denied responsibility. [61]

## *Infrastructure Threats*

Nation states often target critical infrastructure in the United States and elsewhere in the world by attempting to breach systems in the electrical, water, gas, and communication industries. Because these infrastructure assets are often connected to the internet, they become attractive targets. Often, the cyberattacks use simple tactics such as email spear phishing to infiltrate infrastructure assets. Sometimes malware is planted and remains dormant until triggered by an outside agency or event. Sometimes ransomware is used to completely shut down operations at the target facility. [62]

## ***Chinese Advanced Persistent Threat***

According to the U.S. Justice Department, the Chinese organization APT1 (Advanced Persistent Threat) is a hacking group that targets individual companies and managed service providers (MSP) to steal intellectual property. By hacking into MSPs, these cyber spies could then break

## Chapter 17

### Nation State Threats

into companies and industries such as banking, biotech, electronics, healthcare, manufacturing, oil, and so on.<sup>1</sup>

According to deputy attorney general Rod Rosenstein, “More than 90 percent of the department’s cases alleging economic espionage over the past seven years involve China. More than two-thirds of the department’s cases involving thefts of trade secrets are connected to China.” [63]

These attacks began with a typical spear phishing attempt. Often, carefully selected individuals at companies received highly targeted Word documents that they were asked to download. These documents appeared to be legitimate, but actually contained remote access Trojans to allow attackers to access and control computer systems. Once they had control of computer systems, these criminals downloaded more software to compromise other systems on the network, escalate their privileges, and search for data. Once the data was found, it was copied to the attacker system, and sometimes the stolen files were deleted from the compromised systems.

In 2015, it was revealed that 5.6 million federal employee fingerprints were compromised in a massive breach of the servers of the Office of Personnel Management. The attack that resulted in the theft of these fingerprints is believed to have originated in China. It was designed to target intelligence and military employees with security clearances. [64] From these stolen fingerprints, the Chinese can identify virtually all U.S. spies and employees of the CIA, NSA, and FBI.

### ***Stuxnet and Other Attacks***

One of the most famous examples of a nation state cyber attack is the Stuxnet worm. This destructive cyber weapon, which was revealed in 2010, is believed to been created by the United States and Israel to directly target the centrifuges used by Iran to enrich nuclear fuel. This extremely sophisticated malware exploited previously unknown zero-day vulnerabilities in the Windows operating system and used these vulnerabilities to infect PCs in Iran.

If the computer infected by the worm was connected to a specific type of programmable logic controller manufactured by Siemens, it altered the programming of the device to cause it to spin in such a way that the centrifuge was damaged or destroyed. The code also informed the controlling computer that nothing was wrong. [65]

---

<sup>1</sup> APT is a type of hacking group that includes nation state attackers. Every nation-state attack is committed by an APT. Groups that focus on fighting nation state groups have nicknamed different country’s APT groups as APT1, APT2, APT3, etc. so they can talk about and follow the groups and their tactics over time.

More recently, there have been cyberattacks against electrical grids and other infrastructure. The United States believes that Russia was responsible for an attack on its electrical grid and the UK believes the Russians attempted to disrupt their infrastructure as well. In 2017 in Saudi Arabia, cyber attackers attempted to cause an explosion in a petrochemical plant.

## *Foreign Election Interference*

It is not uncommon for governments to attempt to influence the elections of other countries. After all, the choice of a leader can sometimes mean the difference between peace and war or victory and defeat. However, the reach of the internet into the homes of virtually everyone combined with the ubiquitous nature of social media has magnified the danger considerably. Russia, China, North Korea, Iran, and other adversaries regularly use social media and other means to attempt to change public policy, influence elections, and generally cause chaos. In 2016, social media platforms such as Facebook and Twitter were used to sow confusion and discord in the American populace. They succeeded in polarizing the election, agitating voters, and misleading the public.

The problem has become so severe that in late July 2020, U.S. National Counterintelligence and Security Center director William Evanina issued a press release warning that foreign adversaries are “seeking to compromise the private communications of U.S. political campaigns, candidates and other political targets. Our adversaries also seek to compromise our election infrastructure, and we continue to monitor malicious cyber actors trying to gain access to U.S. state and federal networks, including those responsible for managing elections.” [66]

## *Threats to Businesses*

Foreign cybercriminals also target businesses directly. In these cases, the motivation usually isn't financial. Instead, the goal is to steal trade secrets, conduct military espionage, embarrass business leaders, and to change or destroy data. They often attempt to collect personal information and money from businesses.

"Nation states are always going to be at the top of [cyber] capabilities," says Jon Condra, director of East Asian Research and Analysis at risk and threat intelligence firm Flashpoint. "They have the time, resources, everything to carry out these types of attacks." [67]

These criminals use sophisticated tools and social engineering to attempt to breach the defenses of a business. They use tactics such as sophisticated spear phishing campaigns to convince individuals within the company to do their bidding.

## *What Can Be Done?*

The difference between cyberattacks by nation states and those by “normal” cybercriminals is that nation states have a deeper pool of funding and support. They are willing to take more time and spend more resources to breach a system because their motivations are entirely different than those by normal criminals. These attacks are aimed directly at specific organizations or individuals of a country. How do you protect yourself against this kind of threat? In late July 2020, U.S. National Counterintelligence and Security Center Director William Evanina stated, “Consume information with a critical eye, check out sources before reposting or spreading messages, practice good cyber hygiene and media literacy, and report suspicious election-related activity to authorities.” [66]

Follow the steps outlined in this guide, especially regarding spear phishing and social engineering. Ensure your staff is well trained and drilled regularly about the dangers and threats, and make sure they understand their role in maintaining proper security.

\*\*\*

Threats from nation states are very real, especially to businesses, the government, and infrastructure. Nation state actors tend to have more resources and motivation to penetrate networks and achieve their goals. Maintaining diligence and keeping your patching and defenses up to date is critical to defeating these types of attacks.



# **Part 3**

## **Countering Cybercrime**





# Chapter 18

## Fundamentals of Safe Computing

As we use computers at work and at home, we're responsible for those systems. One of the best ways to fulfill this responsibility is to act as good cybercitizens. This means becoming educated on best practices for **safe computing** and executing them diligently.

This chapter examines safe computing practices at the user level (on desktops and laptops), on networks, and beyond.

### *What Does Safe Computing Mean?*

**Safe computing** is the application of safeguards and precautions that protect you from becoming a victim of cybercrime. To ensure that you're safe from cybercrime—or at least safer—you must educate yourself and your employees about the dangers and threats that exist online.

Becoming aware of various options to secure systems—such as using encryption, complex passwords, and physical security—allows you to select and use multiple layers of defense. The more layers of defense you can erect and use, the safer your computing experience will be!

*It's just as important to use protection tools and techniques as it is to understand what types of attack may come your way on the internet.*

Fraudulent activity can originate from the internet or internally on your own networks. You should know how to recognize and respond appropriately to attacks, regardless of their origin. Also, by arming yourself with the proper protective tools, you can mount a more effective response. Ultimately, learning and understanding how to recognize and counter cybercriminal methods and techniques is essential to practicing safe computing.

### *Best Practices for Safe Computing*

You can employ many methods to create a safer computing environment. In this section, we'll discuss some of the most effective best practices. If you apply them correctly and consistently, you can mitigate the risk of successful attacks and criminal action. This list is by no means exhaustive, but it does include options for various situations.

## Chapter 18

### Fundamentals of Safe Computing

Most of these best practices for safe computing bridge the gap between home and work environments. Certain concepts, such as using strong passwords, apply in both cases. Others may make sense only in one world or the other, such as network protection, which is too expensive to implement on most home networks but typical on organizational networks.

### **Physical Security**

A common idiom states, “Possession is nine-tenths of the law.” In the case of cybercrime, possession typically allows for abuse of the law. It’s often said that if an attacker has unrestricted access to your computer, he owns it and there’s nothing he can’t do. If thieves take physical possession of property that doesn’t belong to them, they have an opportunity to exploit that property for gain.

It’s very difficult to protect something that’s not in your possession. If a thief steals your laptop, for example, you can’t directly protect that laptop. Hopefully, you took measures to protect information on the system, such as using a login fingerprint scanner, backing up data regularly, using encryption, and installing a tracking program or chip. Many people don’t. A thief will go to work quickly, using several software programs to obtain login access to the system. If the laptop contains sensitive financial information, such as bank account or credit card numbers, the criminal hits the jackpot once a login is achieved. To reduce the opportunity for physical manipulation and, in turn, theft, you need to take measures to establish physical security.

**Physical security** comes in many forms. One of the simplest forms is a lock and key. In larger organizational environments, IT staff typically keep servers in locked server racks, in locked server rooms. By limiting who has physical access to the machines, you reduce the opportunity for physical theft.

In both cubicles and home offices, a lot can be said for storing laptops in locked cabinets when you’re not using them. Also, most laptops ship with built-in locking ports that let you attach laptops to desks or racks. You can purchase aftermarket locking devices to secure workstation and desktop machines, too. By maintaining physical control over hardware, you make it more difficult for criminals to obtain access to data. If they must use the network to get to a computer, protection is more easily implemented because the point of entry is narrower. (You’ll learn about network safeguards later in this chapter.)

#### ***The Merits of Logging Off***

*Another method for protecting systems is to enable and enforce account logoff or machine locking once a specific idle period has elapsed. This ensures that a hapless user doesn’t become victim to a criminal because that user left a workstation logged in and unattended.*

*If an attacker gains physical access to a machine that's still logged in but not in use, the hard work required to access the system is already done. Getting to the good stuff—the data—is usually easy at this point. That's why automatic lockout or logoff is such a good idea and an important part of safe computing practices.*

## Passwords

The primary authentication mechanism used in computing today is account names with associated passwords. Authentication is the process of identity verification, which can take several forms. A username and password combination is a simple form of authentication. These credentials are pieces of information a user must know to be successfully admitted and granted access to resources in an environment.

A user who presents a valid username and password for authentication validates their digital identity. Using only a username and password combination for this validation is an example of **one-factor authentication** or single-factor authentication. This is because only a single form of identification (the username/password combination) is requested and validated for granting resource access. Using additional verification methods improves security.

### ***And You Are . . . ?***

*Authentication applies to everyday life as well as the computing world. Let's say you call a plumbing company to request service for leaky pipes. When the plumber knocks on your front door, you might notice that he's wearing a uniform representing his employer and maybe driving a company truck or van. If you're still not convinced, you might ask to see his company ID or driver's license. Then you would let him in. Each of these activities serves as identity validation and helps prevent the social engineering practice of impersonation.*

Two-Factor Authentication requires two types of authentication to successfully logon. 2FA can include something the user knows, such as a password, as well as something the user has, such as a smart card, a USB access token, or a text message sent to a cell phone. **Multi-Factor Authentication (MFA)** requires two or more authentication factors to be used to successfully log on. Some high-security environments may require biometric identification (such as a fingerprint, retina vein, or hand geometry scans) along with other authentication factors to allow a successful logon.

*Multi-factor authentication is highly recommended but is not perfect. It can still be hacked. You can use the complimentary **Multi-Factor Authentication Security Assessment (MASA)** at <https://www.knowbe4.com/multi-factor-authentication-security-assessment> to determine the strength of your MFA solution and learn the many ways it can be compromised.*

## ***Using Secure Passwords***

These days, we need passwords for just about everything: logging in to a computer, accessing corporate resources at the office, or banking online and checking personal email at home. With cybercrime on the rise, and because of the growing portfolio of passwords we must constantly manage, it's increasingly important to ensure that people use safe passwords and use different passwords on every website and service.

The function of passwords in any corporate, personal, or internet computing environment is to provide easy-to-use security during identity verification. To improve the strength of a password, you must consider its characteristics. Just as "loose lips sink ships," poor passwords can inadvertently grant attackers access to private resources.

There are several characteristics of a strong password:

- ✓ Is at least twenty characters long
- ✓ Contains a combination of numbers, letters, and symbols
- ✓ Contains a combination of uppercase and lowercase letters
- ✓ Is not a common name or username
- ✓ Is not a word in the dictionary of any language

Passwords hold the key to data access. Whether a password protects a single file or is used in combination with a login name, you're only as safe as the strength of your password. The longer a password stays the same, the greater the chances that an attacker will learn the password and steal information. It's considered a best practice by many security experts to force users to change passwords regularly. The same principle applies to home offices and password-protected websites. Because the latter is usually not enforceable, encourage your employees to take it upon themselves to change their passwords frequently.

**Password safety** must be taught for users to understand appropriate password usage habits. Some key concepts you should communicate to employees include the following:

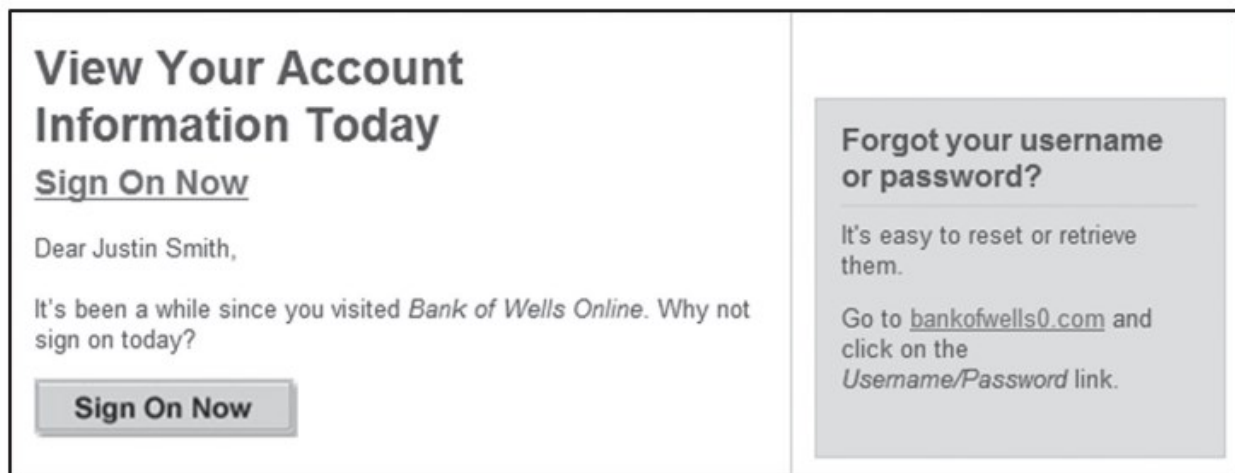
- ✓ Change your passwords periodically—at least once a year.
- ✓ Choose strong passwords that are difficult to guess.
- ✓ Use different passwords for every site and service.
- ✓ Do not use personal information such as birthdates, addresses (in part or whole), children's names, pets' names, and so on.
- ✓ Do not share your passwords with others.
- ✓ Do not write down passwords. Instead, use a password manager or phrase techniques to create a strong password that is easy to remember.
- ✓ Do not keep a password file on your computer.

- ✓ Never use public computers access password-protected websites.
- ✓ Never put your password into a website or service not protected by HTTPS/TLS
- ✓ Never respond to email requests for your password.
- ✓ Use a password manager.

Phrase techniques produce strong passwords. One technique involves creative transformations for a sentence so that, for example, “I never eat rye bread” becomes iN3V3RtaeWRYdearb. Another technique uses creative abbreviations, turning “I have two left feet and crossed eyes” into IH2lf&x0><0. Such passwords are fairly easy to remember yet nearly impossible to guess.

## Social Engineering and Phishing

Social engineering is one of the most problematic attack techniques to combat. It preys on our nature as human beings and is therefore difficult to counter by using technology. User education is most effective at stopping a social engineer. Users who are aware of the potential for social engineering attacks and learn to recognize them can use simple methods to thwart these attacks successfully. As described in Chapter 1, phishing is a type of social engineering that’s executed through unsolicited email messages. Figure 44 shows a sample phishing email message.



**Figure 44** An example of a fictitious phishing email

Notice that the email message looks as if it came from the user’s bank. The formatting most likely matches that of the bank’s typical email messages. The name of the bank looks correct, and the user’s name even looks properly addressed in the message.

At first glance, this email message looks legitimate. It appears as though the bank sent it to ask the customer to log in to his account. However, notice that the link provided on the right side of the message has an extra 0 in it. If you hovered your mouse pointer over the Sign On Now button, you would discover the same thing. The email message did not originate from the bank. It’s

## Chapter 18

### Fundamentals of Safe Computing

actually intended to direct the user to a malicious website. The look and feel of the rogue website would be similar to the look and feel of the actual banking site, but a criminal, not the bank, would receive any data the unwitting user entered.

With the user's name and password, an attacker could go to the real banking site, access the victim's account, and steal money. If the victim uses the same username and password on many sites, the cybercriminal has also obtained credentials to many of that person's accounts. The results could be catastrophic for the victim. Damage could range from petty monetary theft, to a complete drain of financial resources, to full-blown identity theft.

### ***Should I or Shouldn't I?***

Users must be educated to understand that it's typically not safe to divulge sensitive information to unauthorized websites, services, or users. For example, users should never respond to unsolicited requests for sensitive information. The request ploy may vary, but the response should remain consistent. Don't do it!

If a user initiates contact, a request for sensitive information could be warranted. For instance, if you call your bank to request a change to your account, the bank first verifies your identity. The bank may do this by asking for the passcode you selected when you established the account. In addition, the bank would ask for other information to authenticate you as a valid account holder, such as your name, account number, and possibly address or phone number.

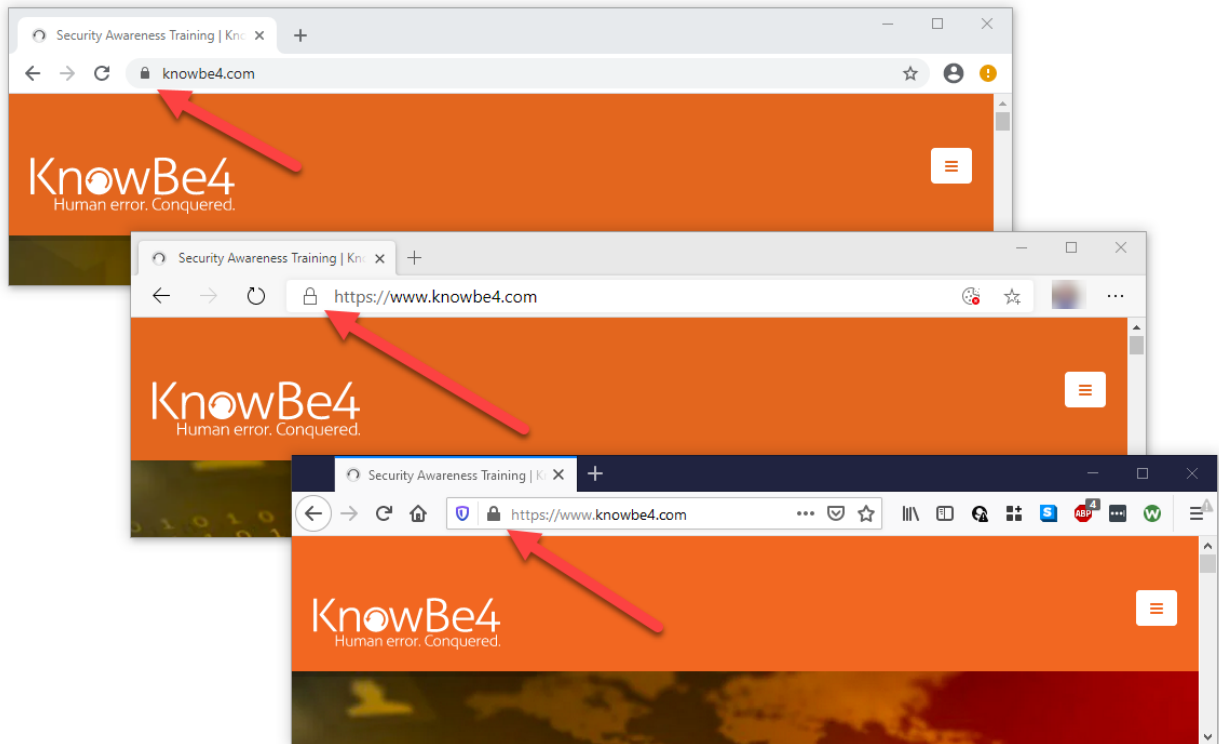
The same concept holds true for websites that are password protected. Let's say you type the address of your bank or email provider correctly in a web browser and press Enter. You can typically be assured that you're connecting to the authentic site. However, if your PC is infected with malware that redirects your web requests, you may still be at risk. This is one reason that an up-to-date anti-malware program is also a must-have for safe computing.

### ***Look for TLS to Keep You Safe***

It's relatively easy to ensure that you're in a secure computing environment. Before entering any sensitive information into a web form, look for an indication of Hyper Text Transfer Protocol Secured (HTTPS)/Transport Layer Security (TLS). TLS is an encryption protocol that, among other things, lets you connect to websites securely. (You'll learn more about encryption later in this chapter.) TLS is the successor to SSL (which is now obsolete) and provides for privacy and protection for data transmission.

*According to the Anti-Phishing Working group (APWG), 74% of all phishing websites use valid TLS certificates. The lock symbol showing that a security certificate is valid cannot be trusted to validate the authenticity of a website. [48]*

Different web browsers display different HTTPS indicators. Figure 45 shows the TLS indicators in Google Chrome, Microsoft Edge, and Mozilla Firefox. Typically, a lock icon is displayed somewhere in the browser screen and the website address is prefaced with the letter's https and a lock symbol. Many browsers (such as Google Chrome) are no longer displaying the https:// text in the URL.



**Figure 45** Lock in Google Chrome (top), Microsoft Edge (Middle), and Firefox (top) (bottom)

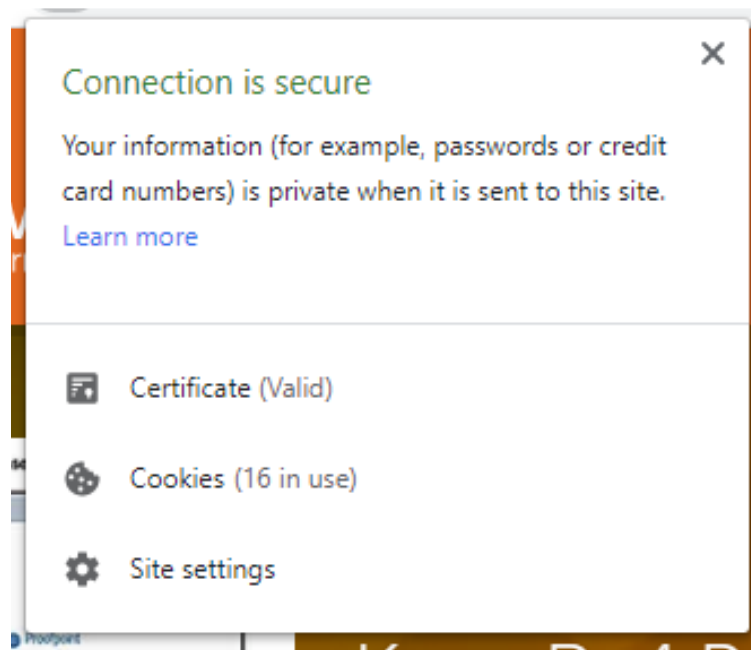
## ***WARNING!***

*Most malicious websites use TLS, as well. Thus, the presence of the lock symbol does not automatically indicate the site is safe. TLS means you have a secure network connection to a website and nothing you type in or send or receive can be easily eavesdropped on. But it does not guarantee the validity of the website you are connecting to or verify that it is safe to use.*

## Chapter 18

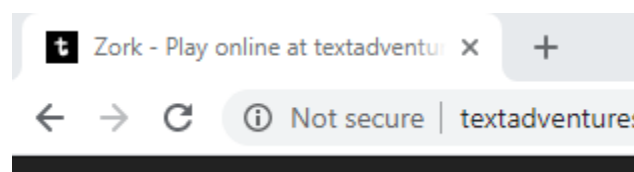
### Fundamentals of Safe Computing

Clicking on the lock symbol will give you more information about the website security, as shown in Figure 46. If there are any issues (such as invalid certificates), they will be displayed.



*Figure 46 Clicking on the lock symbol to find out about site security*

If a connection is not secured with HTTPS, it transmits data across the internet as **clear text**. Clear text is unencrypted text that can be read by anyone who captures the transmission. A website without a valid TLS connection will be shown as insecure by most browsers, as shown in Figure 47.



*Figure 47 Insecure site indicator*

# WARNING!

*Never enter any sensitive information into a website before checking the web browser for some definite indication that TLS is in use.*



If you have followed best practices and taken safety precautions, you may decide to follow through with an online activity anyway. However, think carefully about what kind of site you're visiting and what kind of information you're being asked to provide. If the URL you are visiting is the correct and legitimate one as you intended and the TLS connection is verified as secure, then you can be assured of safe and secure communications to that website. Still, just relying on TLS alone, you can't be assured that you are connecting to a safe website or that a legitimate website hasn't been previously compromised and is waiting for a victim to visit. In some circumstances, you should be skeptical and suspicious. If you doubt the legitimacy of any situation, refuse to provide sensitive data to the requesting party. A cybercriminal could be trying to trick you into providing private information.

## **Network Security**

An internal network is a common attack point for cybercriminals. Data being transmitted locally from point A to point B is typically sent unencrypted. This allows an attacker who's eavesdropping to capture a copy of the data and read the contents. **Defense in depth** uses multiple layers of security in a network. For instance, instead of allowing users from the internet to directly access your internal network, you would implement a firewall. Firewalls are hardware devices or software that restrict the types of traffic that may flow into, through, and out of a network, device, service, or application. Firewalls use rules to control network traffic flow. You create a specific list of rules that allows only certain types of network traffic past the firewall and it blocks all other traffic.

By using components such as proxy servers, you can further extend network control to web-based traffic. A proxy server can block access to particular websites and services for users within a network or host. When a proxy server is deployed, administrators configure workstation web browsers, such as internet Explorer or Firefox, to send all website requests to the proxy server. As a result, the proxy server acts as a gatekeeper for requests and can selectively allow or deny access to specific destinations.

You should also enforce **access controls** (of which authentication is a part) and minimize the permissions (level of access) granted to users for system resources. Grant users and administrators the lowest level of access required to perform their job functions and no more. This is referred to as the **principle of least privilege**; access controls and least privilege are covered in Chapter 20. Firewalls and proxy servers, along with user access control, are common components of a defense-in-depth strategy.

Encryption is the process of making clear text unreadable using cryptographic methods. Before anyone can read encrypted text, it must first be decrypted. By encrypting sensitive data wherever possible, you greatly reduce opportunities for unauthorized parties to steal sensitive information.

## Chapter 18

### Fundamentals of Safe Computing

Network administrators and attackers alike use a network tool commonly referred to as a **sniffer**, **packet analyzer**, or **protocol analyzer**. This tool captures network packet data transmitted across a cable or wireless connection and lets the user analyze any unencrypted data to determine its payload. Unlike clear-text data, encrypted data that's captured by a sniffer is difficult or impossible to read.

As you learned earlier, TLS is an encryption technology that greatly contributes to safe computing on the internet. By securing transmissions using TLS from web browsers to web servers, information such as credit card numbers and social security numbers can be transmitted in an illegible format, therefore enhancing protection. Consider encrypting data on the internal network as well for a very high level of security.

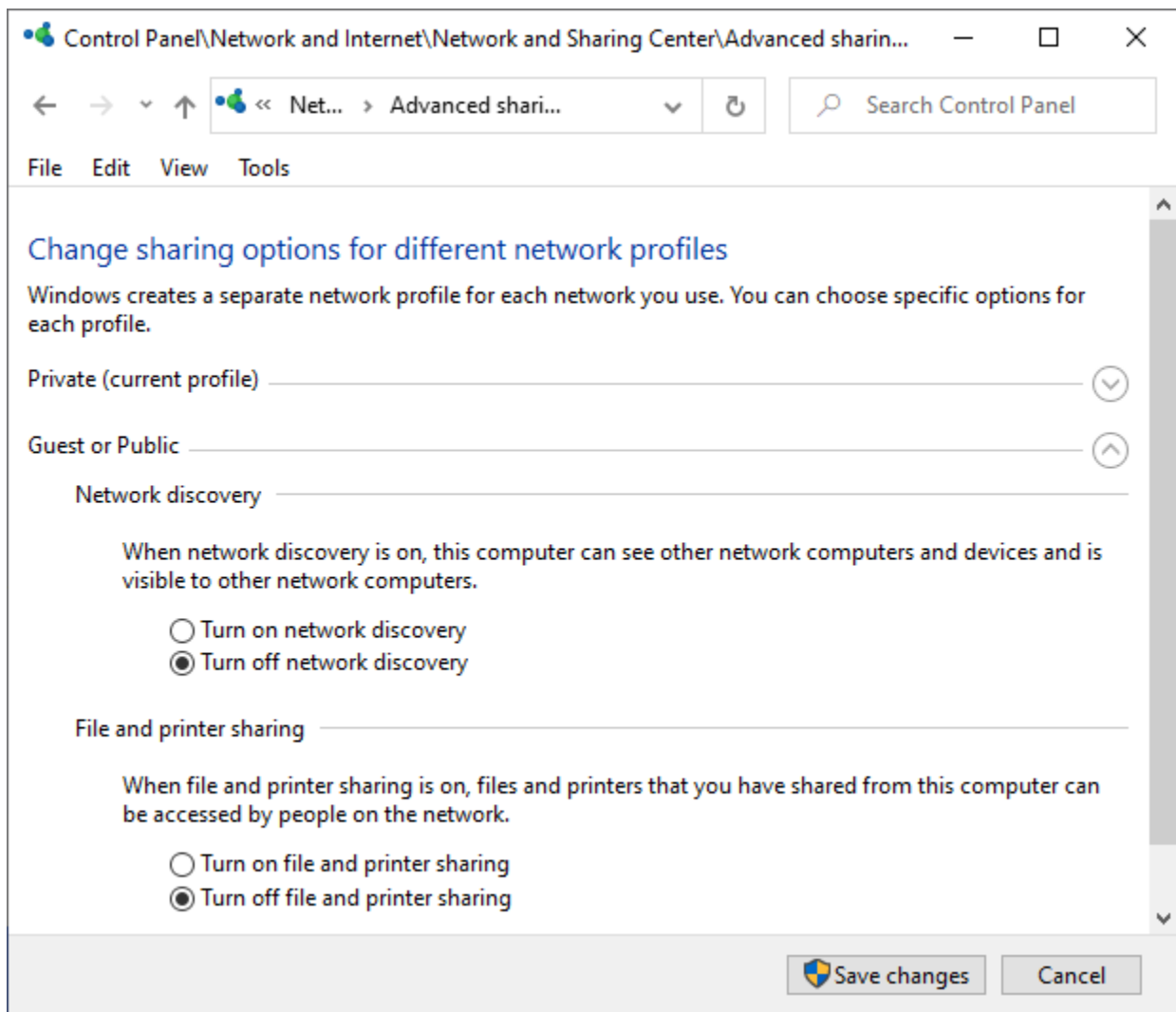
### ***Public Use of Private or Public PCs***

**Public PCs**, such as computers in libraries or internet cafes, present a high security risk to users. Public use of private PCs is common in airports, hotels, and coffee shops, and it has similar risk as using public PCs. The security of the PC and its internet connection are out of your control. An attacker can install malicious software, such as a keylogger, on the PC to capture typed in usernames and passwords. A packet sniffer may even be running on the network, capturing your internet activities. All you have to do is access your bank or a similar website from a compromised public PC, and your credentials can be stolen in seconds.

By connecting your laptop to a public network, such as free Wi-Fi, you're taking on all the risks that come with an unmanaged, open network. Attackers often set up free Wi-Fi networks in public places to lure unsuspecting victims. Once you connect to the rogue Wi-Fi network, the attacker may intercept your emails, get your usernames/passwords, or execute a malicious attack on your computer. You most likely won't notice a thing.

So, if you need to connect to a public Wi-Fi network, ensure that you're clicking a valid and safe network name. At the airport, look around for a sign that advertises the Wi-Fi network. At a coffee shop, ask the barista. Do not attempt to connect to any other available Wi-Fi networks in the area. Make sure your PC's firewall is on, lock down your public wireless connection settings (see Figure 48), and encrypt sensitive files or folders on your hard drive ahead of time, if possible.

*If you don't need internet or network access, but just want to use your PC, you can shut off your wireless connection. This can usually be accomplished by changing a software setting, although some devices also have a physical selector switch.*



*Figure 48 Turning off network options on Windows 10*

## Antimalware

Recall from Chapter 1 that malware is any software that's installed on a computer with the intention of executing malicious code. Typically, the software installs without the owner's permission or without the owner being aware of its true intentions. Malware comes in many forms, including viruses, worms, Trojans, spyware, and adware. The best protection against malware is to install antimalware protection software, and safe behavior. Antivirus and antispyware software comes in stand-alone packages or as part of full-featured suites. Regardless of which software you select, it's important to take these two key steps:

- ✓ Always ensure that the software is up to date.
- ✓ Never circumvent critical default security protection mechanisms.

## ***Safe Internet Use***

Safe internet use starts with using safe computing habits while surfing the internet. **Safe surfing** refers to a user's behavior when browsing the web. Cybercriminals will try many different ways to get sensitive information or take your money in a scam. You have to watch out for their tactics.

### *Watch What You Download*

First, avoid questionable downloads. Never click on a pop-up or pop-under ad when using a web browser. Although some are completely harmless, most are not. Many people fall for "optimize your PC" or "disinfect your PC" pop-ups. Clicking such ads guarantees a rogueware (spyware or other malware) infection on your PC.

Also, scrutinize any software you intentionally download from the internet. The enormous amount of free software on the internet is tempting, but it's best to visit the vender's website directly. Clicking just any link that comes up in a list of search hits can have devastating effects.

For example, say that your coworker gives you a web camera he no longer uses. You attach it to your PC, but don't have the software to run it. You search the internet, click the first link at the top of the results list, download software, and install it. After a few days, your PC seems sluggish, and the hard drive seems to be working overtime. You run an antivirus scan, which finds a handful of malware programs. If you're able to quarantine the malware without losing data or your passwords, you're lucky. More likely, by the time you detect the malware, your PC has been compromised for days or longer—along with your bank and credit card accounts.

### *Don't Click Any Ol' Link*

We've said it countless times in this book because it's so important: Never click links in unsolicited emails or on suspect websites. Email from a trusted source is generally safe. However, ensure that the email is actually from the trusted source and asking for a valid action before taking action. Even email from trusted sources can sometimes contain maliciousness if the source was previously compromised without you knowing it. Chapter 1, Chapter 3, and Chapter 4 dissect some other phishing examples to help you avoid scammers and attackers.

### *Verify the URL Domain*

The single best thing anyone can do before clicking on a URL, whether it is protected by HTTPS or not, is to verify that the domain name (e.g., knowbe4.com, microsoft.com, paypal.com, bankofamerica.com, etc.) is valid and legitimate for the claimed brand or vendor. Users should always "hover" over a URL link before clicking on it and verify that the domain name is legitimate and not some unrecognizable or trick domain that will take them to some other potential malicious web page. For more information on how to spot a rogue URL, see: <https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks>.

*Individuals and organizations should use spam and content filters to reduce the amount of malicious email and content. Internet email providers usually have built-in spam- and content-filtering tools you can use and configure to meet your needs.*

\*\*\*

To practice safe computing, you must apply safeguards and precautions that protect you and your business from becoming a victim of cybercrime. Educate yourself and your employees about the dangers and threats, and be ware of options such as encryption, complex passwords, and physical security.



# Chapter 19

## Syncing Up Security Policies, User Training, and Monitoring

To some extent, establishing and maintaining proper information security is a balancing act. It involves formulating security policies to state what assets are worth protecting, how far such protection should go, and what kinds of protection should be applied to them. User training helps to address the all-important human element in security. Finally, monitoring is necessary to ensure that security is working and protecting the right things. It also enables organizations to react quickly and decisively when a security breach occurs.

This chapter addresses security policies, user training, and monitoring, aimed at protecting small to medium enterprises (SMEs). Failing to implement even one of these components can greatly increase your organization's risk of attack or security breach.

### *Security Policies*

A **security policy** is a document that establishes how an organization secures its facilities and information technology (IT) environment. Large organizations may have several policies, in separate documents, that represent a collective security policy.

The more complex the policy, the more difficult it is to maintain. In an SME environment, a best practice is to designate one person to be in charge of policy maintenance. That person can assign parts of the policy to different personnel, but he or she should be aware of all policy changes and any ripple effects.

The physical security of all things IT, such as switches, routers, and servers, must be addressed. In addition, the policy should outline protection methods used to safeguard IT assets from unauthorized access and exploitation. It should also address the actions administrators and security personnel will take if a security breach occurs.

### ***Why Security Policies Vary***

Every organization is unique, and even departments within the same organization might face different threats. This leads to security policies varying greatly among organizations. For example, many of the components in a security policy created at a university may be appropriate for use

at a large company. However, the same policy components may be too complex for a very small business or a nonprofit.

## ***Creating and Enforcing Security Policies***

Security policies should be based on the requirements of the organization. These requirements may be departmentally based or may vary across units within the organization. An initial step in security policy creation is to collect and validate business requirements. The next step is to create components in the policy that successfully address each business requirement.

Once its security policy is in place, an organization must be able to enforce it. Effective enforcement starts with user training and awareness. Buy-in from employees is particularly important for policies to be successful. Additional methods include auditing and monitoring. Without enforcement and clear ramifications that result from policy breaches, a security policy becomes little more than a piece of paper.

## ***Adaptability Is Key***

Because the needs of an organization change over time, a security policy should remain adaptable to support changes as technologies change. In smaller environments, fluidity may exist, but resources may not be readily available to keep up with the implementation of a well-documented security policy. On the other hand, large organizations often have adequate resources, but lack the flexibility of smaller entities.

*You should review your security policies regularly to ensure that changes in technology haven't invalidated the policies or require changes in the policies.*

## ***Parts That Make the Whole***

All organizations—regardless of size or industry—have similar goals for achieving a more secure environment. A security policy helps secure the environment by documenting perceived risks and outlining mitigation plans. Security policies normally have multiple components, including the following:

- ✓ **Acceptable use policy:** This policy addresses network and internet use as well as acceptable user behaviors and activities.
- ✓ **Enforcement policy:** This policy spells out how, when, and why security will be implemented in the environment, potentially including actionable consequences for breaching the policy.
- ✓ **Monitoring policy:** This policy specifies monitoring activities that are required. It also indicates who and what is monitored and at what frequency.



- ✓ **Physical access policy:** This policy specifies the physical resources to which users are granted access; it also includes information regarding the circumstances and mechanisms of authentication.
- ✓ **Educational policy:** This policy addresses the methods and frequency of user training.

The security policy might also address intrusion protection requirements, disaster recovery requirements, incident handling, authentication requirements, and more.

## ***An Example of a Security Policy Outline***

The following is an example of a simple security policy outline (without any detail). If you don't already have a security policy in place, you could use this structure to get started. Just modify it for your organization:

- Policy statement and introduction
  - General information
  - Objectives
  - Responsible organization's structure
  - Security standards
- Antivirus protection
- Physical security
  - Definitions
  - Required security
- Access control system
  - Identity Management
  - Authentication
  - Authorization
  - Access controls
- Network and perimeter security
  - Wired
  - Wireless
  - Firewalls and perimeter devices
  - Internet
- Server security
  - File servers
  - Web servers
  - Database servers
  - Cloud servers
  - Print servers
- Workstation security
- Mobile device security

## Chapter 19

### Syncing Up Security Policies, User Training, and Monitoring

- Email systems
- Telecommunication systems
- Security services and procedures
  - Auditing
  - Monitoring
- Computer security incident handling
- Contacts and other resources

For each section of the outline, you need to fill in details that describe the security measures in your organization. However, your policy should not be so detailed that it becomes inflexible and difficult to update. The policy language should be clear, concise, and must be understandable by all users.

*You can find a wealth of sample security policy templates at the SANS Information Security Policy Templates website. Visit [www.sans.org/security-resources/policies/](http://www.sans.org/security-resources/policies/).*

### A Closer Look at Acceptable Use Policies

Imagine that you're working on a team project and have some important deadlines approaching. One member isn't getting her work done on time but assures everyone that she's "on it." Every time you glance her way, she appears to be occupied. Finally, you walk past her desk and notice that she's on eBay, browsing auctions. At lunch, you try talking to the team about the upcoming deadlines, but your coworker interrupts with "Did you see the dancing granny video on Facebook this morning? What a hoot!" You're fed up, but not really sure what you can do. The good news is that there may be a simple way to address this type of behavior. Most organizations create **acceptable use policies (AUPs)** that help managers enforce appropriate internet usage.

An AUP outlines the rules of the road for accessing and using an organization's computing resources. To some of us, documenting acceptable computing activities and behaviors may seem like a reiteration of common sense. However, a surprising number of people abuse their privileges at work every day. A well-written AUP outlines appropriate usage and the consequences of disregarding the rules, including disciplinary actions that may be taken by an employee's manager.

In addition to using an AUP to regulate employee behavior, an organization might establish an AUP for legal protection. If an employee's behavior consists of a criminal act resulting in litigation, an AUP can help protect the employer. The AUP demonstrates that the organization did not support the employee's behavior. It establishes what is expected of employees and helps confirm that the employee was acting on his or her own accord, in violation of the policy.

Also, organizations that create AUPs and require staff to follow them offer fewer opportunities for cybercriminals to exploit the environment and steal data. AUPs are designed to promote safe

and appropriate user behavior, which greatly reduces the likelihood of legal proceedings that may result from data theft or other crimes. After all, business suffers when key employees are tied up fighting legal battles—unless you’re an attorney!

## **What’s in an AUP?**

When an SME decides to establish an AUP as part of its security policy, the organization typically includes guidelines for using IT assets and performing computing activities. The AUP describes usage rules for systems and networks. For example, the AUP may address web browsing, instant messaging, and checking email, providing examples of acceptable behavior. It may also describe role-specific activities—for example, for users, managers, and administrators. Or it may prescribe acceptable use for the entire user population, regardless of role.

*Regularly remind users about AUP details using login banners, routine training, and annual reviews with signed acknowledgments.*

An AUP must also include the consequences of not adhering to the policy. Users must understand why they need to take an AUP seriously. With repercussions in place for violating the policy, the AUP becomes a much more formidable force. This is especially true in organizations where some users are transient. Universities, temp agencies, and companies that hire seasonal help have a significant number of users rotating in and out within a short time. The monitoring component of a security policy is especially critical in these organizations. Without monitoring, inappropriate user activity goes unnoticed. Also, with steeper repercussions and consistent enforcement, it’s easier to encourage appropriate behavior.

*The AUP should clearly state the consequences of breaching the policy. In addition, it’s important that penalties are appropriate. For example, a user caught reading personal emails during work hours might receive a warning for a first offense; a user browsing pornography at work might be terminated. In many instances, the language of the AUP needs to be detailed and/or precise to properly address correct and incorrect behavior. Let’s say your organization’s AUP states that employees may not use Twitter. However, an IT employee follows a Microsoft Press author on Twitter to keep up to date on emerging technologies. In this case, a manager may be reluctant to discipline the employee. If the manager then disciplines someone else for personal Twitter use, the manager can be accused of inconsistent enforcement of the AUP.*

In some cases of breach of the AUP, an organization’s human resources department may need to get involved. Some situations may even be serious enough to involve the local authorities. Breaches of all sorts can happen in any organization, and it’s important to be prepared for such situations. An AUP must be clearly written and thoroughly documented. It must also adhere to any local, state, and federal laws that apply.

### ***An Example of an Internet Use Statement***

*The following is a portion of a sample internet use statement that may be included as part of an AUP and could be further expanded to meet an organization's needs:*

*"Corporate assets are allowed to be used to access the internet for business purposes only. Internet access from corporate equipment for non-business purposes is strictly prohibited. Accessing gaming sites, social networking sites (Twitter, Facebook, YouTube, Instagram, and so on) for personal reasons, or pornographic or other sexually explicit materials on the internet from corporate assets is strictly prohibited. Any internet access that falls outside the bounds of business-specific behavior is considered a breach of policy. Failure to comply with this stated policy will lead to disciplinary action of the employee. Repeat offenses may lead to work suspension and possible termination of employment."*

## **User Training**

"I didn't know." These three simple words have led to severe security breaches in organizations large and small. User education and security awareness can stop most threats, including those launched by cybercriminals. A security policy is an organization's blueprint for safe computing. When it's followed, it acts like a shield against scammers. A policy stands a greater chance of success when everyone understands its importance and buys in to its terms. Employees need to understand why the policy is necessary, how to adhere to it, and what will happen if they don't. This is what security policy training is all about.

*To get a security policy off the ground, management must agree that the policy is necessary. Then, managers must set an example by adhering to the policy.*

Employees won't be interested in training that focuses only on consequences and penalties. They need to understand what can happen to the organization—and potentially their jobs—if a major security breach occurs. Presenting problems from their perspective can help you gain their support. It's also helpful to remind them that security can be very simple—that many security issues can be avoided by thinking before clicking.

Organizations change, and policies change, too. When changes occur, more training is needed. Therefore, an organization might consider offering security policy training in phases:

- ✓ **Entry-level or introductory-level training** for users who are new to the organization
- ✓ **Periodic refreshers**—perhaps quarterly or annually—to keep the users in touch with the security policy
- ✓ **On-demand training** as new scenarios or changes to the policy occur

## ***Break Out the Surveys***

**Surveys** can help ensure that users are learning from and supporting training efforts. You can ask users for feedback informally, such as through email or in person at the end of a session. Some organizations require employees to take a test or provide formal feedback at the end of training. An organization might keep training attendance, test results, and feedback as part of the employees' records. Regardless of the approach, you need a way to determine whether the training was effective. Frequent simulated phishing attacks are an effective way to do this.

Feedback can show you when you need to adapt training to meet the needs of any employees. Trainers can use feedback to improve and customize the training experience. Customized training leads to a more thorough understanding and adoption of the security policy.

## *Monitoring Techniques*

After you've implemented a security policy, you need to ensure that it's having the desired effect. Ideally, you will want to validate all aspects of your security policy. This means that your validation and monitoring plan should not only include things such as checking for unauthorized access attempts into secured building areas, but also recording and being alerted to unauthorized file access on the network.

To check on the state of your physical environment, you can conduct premises monitoring. **Premises monitoring** is the practice of monitoring multiple physical aspects of your environment. This may include but is not limited to areas such as:

- Parking lots
- Lobby and public waiting areas
- Unsecured employee areas, such as where receptionists or temporary workers are housed or conference rooms, cafeterias, and restrooms are located
- Secured employee work areas, such as an area where only authorized employees have been granted access
- Secured resource storage areas, such as datacenters and wiring closets

Why is physical security so important? Having physical access to a system gives an attacker a distinct advantage. For example, to access a network from the outside, an attacker has to traverse multiple firewalls, including network firewalls and host-based firewalls. Then he or she has to deal with authentication requests and prompts. If the attacker gets into the network, he or she might have to get past permissions configured on specific files and folders. However, acquiring physical access to a system on the network negates most of these protection mechanisms.

## Chapter 19

### Syncing Up Security Policies, User Training, and Monitoring

An attacker who gets physical possession of a system can boot the system from a CD or universal serial bus (USB) drive and then gain administrative access to the entire system. The attacker can then reset passwords, destroy, or steal data, and format the system before moving on. An attacker may also choose to disrupt system activities by forcibly rebooting machines or installing undesired hardware or software such as keyloggers. Premises monitoring can help you prevent cybercriminals from accessing your systems.

A premises monitoring system may consist of multiple devices and monitoring systems, including the following:

- **Video cameras:** Before attackers can get to the computer systems in a data center, they must gain physical access to the building. Video cameras in parking lots and driveways allow you to track people entering the premises.
- **Door security:** To keep the systems in a facility secure, the doors to the facility must be secured. Oftentimes when public access is granted to a facility, the entrance allows all visitors access to a sealed lobby area. Doors leading from the lobby to the user work areas and beyond are secured. Individuals who are allowed through those doors are admitted by a security guard or a technology such as card readers or keypads.

Do security guards or technologies provide better physical security? It depends. Certainly, it is possible for attackers to steal key cards or other credentials to bypass either type of security. However, when a security guard is responsible for granting access to the inside areas of a work environment, there is an increased chance of successful attacks using social engineering. An attacker might be able to sweet talk a night guard into granting access to a building, using a cup of coffee and a smile. Such tactics simply don't work with an access keypad.

### ***Tracking User Activity and Behavior***

Regularly reviewing access logs for sensitive areas can help an organization observe patterns of behavior. If a user repeatedly tries to gain access to the server room but his badge is denied access, this may be cause for concern. Similarly, an organization needs to keep track of who should have access to secure areas and who no longer needs it. For example, it's important to revoke access to secure locations once an employee leaves a department or the organization.

Something else to be aware of is **tailgating**. In environments that require card readers for door access, some users find it a nuisance to swipe their identification card in the reader every time they enter. So, employees start holding the door open for the person behind them or a following user may enter right behind a user in front of them. Tailgating is one of the primary access methods for unauthorized users, and social engineers use it all the time. Why wouldn't you hold the door for the guy wearing a delivery uniform? A social engineer simply waits for an authorized user to open and pass through a secure entry—and then follows right behind. Criminals rely on the polite tendency to hold the door for those behind us.

## Chapter 19 Syncing Up Security Policies, User Training, and Monitoring

\*\*\*

Educated users who respect and follow a security policy greatly reduce the opportunities available to social engineers and cybercriminals. As with most other security measures, user training is key. When they understand the rationale behind a policy—and understand the policy itself—users are more likely to comply. This compliance leads to safer, less vulnerable environments and fewer successful cyberheists.





# Chapter 20

## Protecting People and Assets with Security Technology

Network and security administrators work feverishly to protect their IT environments from attackers and other threats. Unfortunately, they must set up mechanisms that protect from inside attackers (disgruntled employees, social engineers, and the like) as well as those on the outside.

In this chapter, you'll learn how to protect your IT environment and your employees with security technology.

### *Information Security Principles and Practices*

**Information security practices** protect people and business assets from threats, including cybercriminals. The three key principles of confidentiality, integrity, and availability are commonly referred to as the **CIA triad**. Here's a quick look at each of these principles:

- ✓ **Confidentiality:** When properly achieved, confidentiality prevents unauthorized access to restricted data in an organization. An organization can enforce confidentiality by implementing access controls, such as authentication and encryption.
- ✓ **Integrity:** An organization needs to validate that data, while in transit or at rest, has not been modified from its original state. Digital signatures and encryption help maintain data integrity.
- ✓ **Availability:** Data and access to data must be highly available and resistant to single points of failure. Data backups, redundant disks, and multiple network connections help ensure availability.

IT professionals can use many different methods to implement the CIA triad. Each organization must evaluate methods to select what's best for its environment.

## Access Controls

To protect IT resources, such as servers, folders, and files, administrators can grant specific access, or permissions, to users and groups. This is accomplished with access controls. An **access control** is a system or technique for allowing or denying access. A door lock is a type of physical access control. Passwords and other types of identification and authorization, covered in Chapter 18, are also access controls. This section looks at controlling access through rights and permissions, in addition to physical controls.

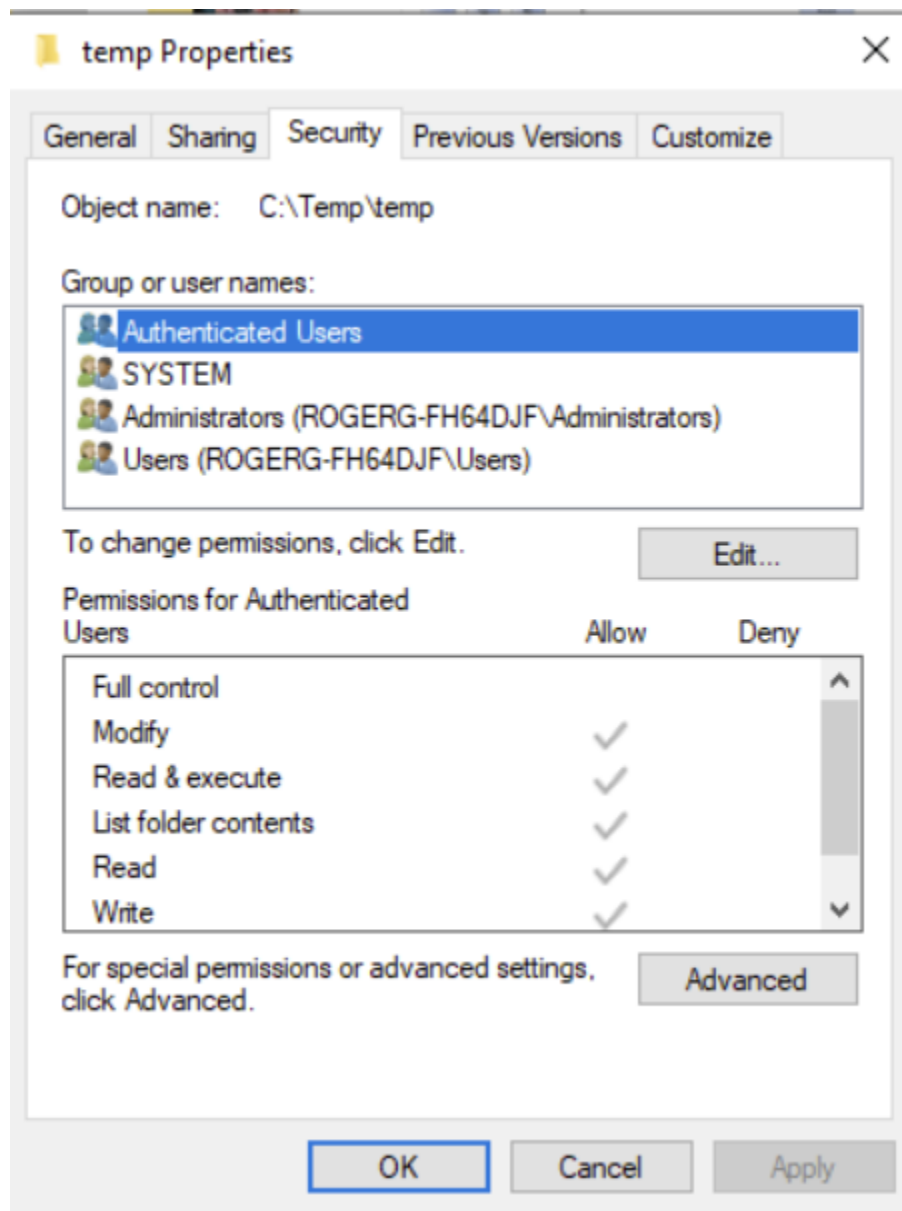
An important concept surrounding access control is the principle of least privilege, which means giving users the least amount of access required for them to complete their jobs. By sticking to the most restrictive permissions required, you reduce the risk associated with mistakes (such as accidental deletions) and unwarranted access.

### Overview of Permissions and Access Controls

Windows systems have two types of permissions: **share permissions** and **NTFS** (file system) permissions. Both permissions come into play when a user accesses a resource from a network. NTFS permissions also apply at the local level, on a user's PC. Share permissions are visible and configurable on the Sharing tab of a file or folder, and NTFS permissions are displayed on the Security tab.

Figure 49 shows the Security tab of a folder named C:\Temp\temp. In the figure, SYSTEM and the Administrators group are the only entities with permission to the folder other than the user or group who owns the folder. Typically, the owner of a resource (file, folder, hard drive, printer, and so forth) controls its permissions, along with administrators. Custom groups and additional individual users can be added to the access control list (ACL). Notice in Figure 49 that both Allow and Deny permissions are available.

*In Figure 49, the owner of the folder is a user account called **Administrator**. This is different from the Administrators built-in group. The Administrators group can contain multiple user accounts. All users who are part of the Administrators group have the indicated permissions simply because they are members of the group.*



**Figure 49** *The NTFS permissions tab for a folder*

It's common to configure restrictive NTFS permissions rather than share permissions because NTFS permissions apply to both network and local access. If both share and NTFS permissions have been configured and the user accesses data from the network, the two permissions types are evaluated together to determine access rights. The more restrictive permission between the two takes effect.

For example, assume that a group named Human Resources has the Full Control share permission to a share named Background Checks. The group also has the NTFS Read permission on the same

## Chapter 20

### Protecting People and Assets with Security Technology

folder. Because Read is more restrictive than Full Control, any user whose account is a member of the Human Resources group will be granted only Read access to the Background Checks folder. Also, because the Read permission is configured at the NTFS level, it would apply regardless of the user access method. If the user connects from the network or locally on the computer that houses the resource, the resulting permission would be the same.

#### *Restricting Electronic Access*

When applying the principle of least privilege to electronic access, such as to computers and networks, you must understand what actions each user is required to perform. Say that a folder named Background Checks exists on a server. The human resources (HR) and legal departments need access to the folder. The Human Resources group is responsible for adding newly completed background check files to the folder. Users in the Legal group only need to read the completed documents. By granting both groups Full Control of the folder, you have met their needs. However, the Legal group has a much higher level of permission than needed.

In this scenario, the users in both groups would be able to edit the files as well as delete files in the folder. Granting the excessive access creates an opportunity for user error—or even for intentional malicious destruction of data. The better course of action would be to grant the Legal group Read permissions only, while the Human Resources group would have Read and Write permissions.

#### *Minimizing Use of Elevated Privileges*

Systems administrators should use an ordinary user account for checking email, researching technologies, and other routine activities. The administrator-level account should be reserved for support and maintenance tasks that require more permissions. Systems administrators require **elevated privileges** (that is, more permissions) to perform certain job functions. But this doesn't mean that all their day-to-day activities require these rights. A user with elevated privileges who is logged in to a computer or the network introduces an increased risk if a device they are logged onto is compromised. If an attack takes over the login session, he or she may be able to exploit the higher-level permissions to do considerable further damage more easily than if a regular user was logged on in.

*Administrators should practice the principle of **least privilege** when configuring access control security permissions.*

#### *Restricting Physical Access*

It's important not to grant blanket physical access to secure locations in your organization. For example, consider a user whose primary role is database administration. The server hosting the database is in a locked server room. The administrator connects to the database remotely to perform maintenance, so he or she never needs to physically enter the server room.

If the company has a blanket policy that grants all IT personnel access to the server room, the database admin would be included in that group. The result is that a person who doesn't require access to a secure area to perform his or her job function has unnecessarily been granted access. This increases the chances for an attack. The database admin doesn't normally work in the server room, so he or she might not know the rules he or she must follow and could inadvertently allow a breach to occur.

## ***Clear-Cut Security Classifications***

**Classifying** data is a way to label it for organizational purposes and to apply levels of security. One way to classify data is by **access sensitivity**. You first create broad security classifications (or categories) and then identify characteristics that qualify data for a particular label. Almost every government agency uses security classifications in some form. The following are some common government security level classification labels:

- ✓ Top secret
- ✓ Secret
- ✓ Confidential
- ✓ Restricted
- ✓ Unclassified

The same concept can be applied to business data. Classifications help administrators label data appropriately and help admins decide which users and groups should have access to the data. Every organization can establish its own set of security classifications. For instance, an organization might use the following data security classifications:

- ✓ Internal—Full access
- ✓ Internal—Restricted access
- ✓ External—Partner access
- ✓ External—Public access

The organization would need to define and clearly document each classification before putting it into practice.

*Some SMEs use the government security classifications but modify them for their own environments.*

Ideally, higher security classifications should be guarded more carefully. Additional security practices may be required to protect the data more carefully in these categories against cybercrime.

## ***Separation of Duties***

**Separation of duties** ensures that one person isn't able to solely handle critical tasks. For example, the person who requests payment of an invoice in an organization should not be the same person able to sign the check. The goal of this separation is to prevent fraud and other illegal activities.

In IT, a software developer might separate operations from development and keep systems testing in yet another compartment. Doing so would reduce the risk of a tester, for example, making unauthorized changes or accessing operations data. Another use of separation of duties in IT is to compartmentalize sensitive functions from non-sensitive ones and use different types of authentication for the two types of functions. Using access controls, an administrator would isolate a critical program and restrict the users or groups that have access to it. In addition, running the program would require a fingerprint scan and password or a token and password. This way, if an attacker wanted access to the program, he or she would need to jump through a few hoops:

- Break into the internal network.
- Learn the credentials of a user who has the appropriate permissions.
- Obtain the proper authentication credentials.

The odds are very low that an attacker will get through all these hoops, making the system very secure against breaches. Separation of duties works well in all parts of an organization, from accounting to IT to HR. By determining which job responsibilities should not be intermingled, HR can work with hiring managers to plan appropriate job roles and responsibilities.

## ***Regular Security Policy Audits, Updates, and Remediation***

As computing environments change, security measures must change, too. In a busy environment, updating security controls and documentation can be put on the backburner unintentionally. Regular security auditing is one way to get everything back on track.

An organization can work with internal departments or hire external companies that specialize in **security auditing** to perform the audits. It should schedule audits according to industry mandates or at least annually. Both management and IT personnel should review the results of each audit.

Thorough audits point to security lapses, holes, and other weaknesses that can leave an SME vulnerable to attackers. An organization should fix any problems uncovered during an audit—to

the extent that its budget allows. The organization may need to spring for technology updates, or it might be able to get away with just changing how employees use the existing assets.

After completing audits, an organization should review its security policies. It should update anything that's out of date or obsolete. Some SMEs must comply with federal or state regulations, so keeping security policies up to date may help avoid penalties as well as security breaches.

*Many audits measure compliance with security policies. They help an organization determine if its security policies are just on paper or actually followed.*

## Using Security Technology

The main purpose of security technology is to protect an entity against attackers and cybercriminals. Cybercrime offers monetary benefits, and frequent attacks against a network and its data are therefore common. The right mix of security technologies and methods can reduce your exposure.

### **Client-Side and Server-Side Security Considerations**

Say that a user decides her locally installed firewall software is a nuisance, so she disables it. Because her computer is connected to the company network, which is protected by a network firewall, she believes nothing can go wrong with her system. Has she made an incorrect presumption? Does her action present a problem to other users and systems on the network? The short answer to both questions is yes. One insecure computer in an environment may not seem like a big deal. But imagine if that computer became infected with a virus or a Trojan and then connected to the network. There is now the potential for a larger-scale security breach.

All clients (which may be workstations or mobile devices) and servers must be well protected. Antivirus software is needed with this strategy, as are firewalls and pop-up blockers. However, antivirus software catches less and less these days. As another measure, lock down workstations and servers by disabling unnecessary services and protocols. If an attacker launches an attack using a service or protocol that isn't installed, the system is protected.

Tightly controlled authentication services, server-specific rights and permissions like those associated with NTFS or Windows Active Directory are also key. Administration of these components can often be centrally controlled, especially in larger SMEs; smaller organizations may prefer local system administration.

### **Public Key Infrastructure (PKI) and Kerberos**

*Some organizations use public key infrastructure (PKI) and Kerberos to provide strong authentication services. PKI is a service which uses **digital certificates** to provide authentication of subjects (e.g., people, companies, and files). The primary job of a PKI service is to verify the identity of a subject before issuing a digital certificate. If a relying party (e.g., person, browser, application, computer, etc.) trusts the “certification authority” (CA) of the PKI service, they will trust the certificate attesting to the subject’s identity when it is submitted to them (or their application). PKIs use asymmetric cryptography, which involves two mathematically related keys: a private key and a public key. The private key is only known by the subject holding it, but the public key can be seen and used by anyone. What one encrypts the other can decrypt; and vice-versa. This allows for encryption and authentication. A digital certificate ties and verifies the subject’s identity to the keys used. PKI is one of the central ways authentication and encryption is done on the internet and by organizations.*

*Kerberos is a network security service and protocol that often provides authentication and authorization services on organizational networks. A Kerberos Distribution Center (KDC) can provide services similar to a PKI CA, but Kerberos usually uses symmetric keys, where the same cipher key is used to encrypt and decrypt data (as compared to the private/public key model of PKI). Both PKI and Kerberos are among the most popular authentication services used by companies to supposedly provide a higher level of authentication security, although this is not always the case.*

## **Securing the Networking Infrastructure**

Most organizations value their data enough to protect it to some extent. Some organizations are more tuned in to security than others. Regardless of the security need, be it simple or extreme, the network plays a key part in achieving security goals.

In most organizations, all traffic to and from the internet must flow through the network. Users access their data files and system resources over the network. Employees and business partners exchange email over the network. Voicemail may be retrieved over the network, and instant messages pass between users across the network. With all the functions made possible by a network, and because the network is a target for attackers, network protection must be strong.

### *Covering All the Access Points, Starting at the Perimeter*

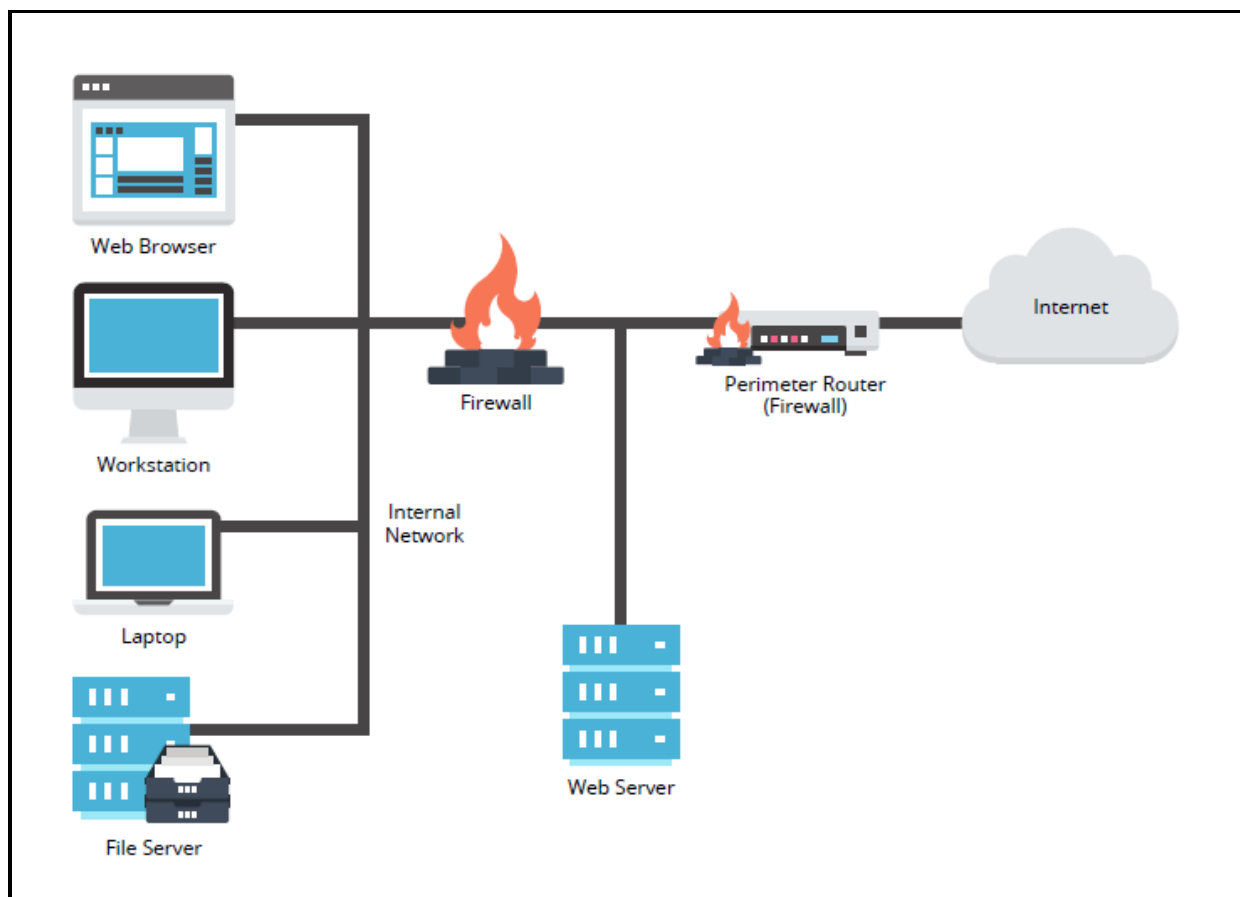
You typically enforce protection at different access points throughout a network. Starting at the perimeter, every network must have a **firewall** (see Figure 50). For instance, internet traffic may flow in and out through a single router. This router should be enhanced, or a firewall added to



protect the network. The firewall can perform traffic inspection or even block specific access attempts.

Adding an **intrusion detection system** (IDS), intrusion prevention system (IPS), and web proxy server strengthens the security of the network perimeter. An IDS monitors network traffic and alerts administrators to possible malicious activity. An IPS goes a step further and may shut down network access when certain malicious activity is detected. Using an IDS or IPS enables you to observe threats, analyze them, and respond quickly.

*Many solutions provide IDS and IPS functionality in a single device or software package. You can also deploy an IDS/IPS on workstations for added security.*



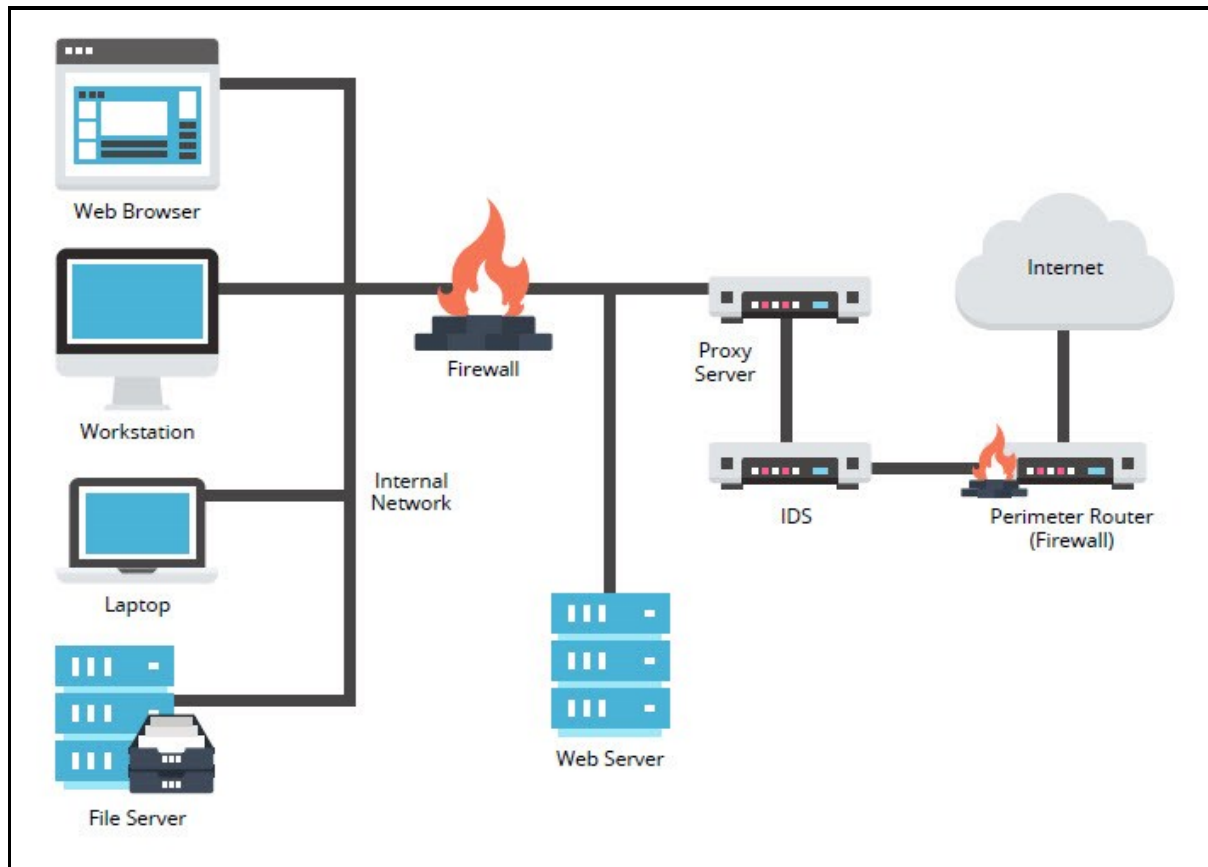
**Figure 50 Protecting the network perimeter with a firewall**

A web proxy server enhances outbound security by filtering the websites that users are allowed to access. For example, if certain web domains are off-limits, the proxy server blocks those domains. Likewise, if certain types of content (video files, music files, and so on) are also off-limits, you can configure the server to block those types of file transfers or attachments.

## Chapter 20

### Protecting People and Assets with Security Technology

You can configure a **web proxy server** (see Figure 51) to enforce the organization's acceptable use policy (AUP) as well as monitor traffic for restricted content. And you can implement an IDS and/or IPS to enhance inbound protection.



*Figure 51 An IDS and web proxy server create a stronger perimeter*

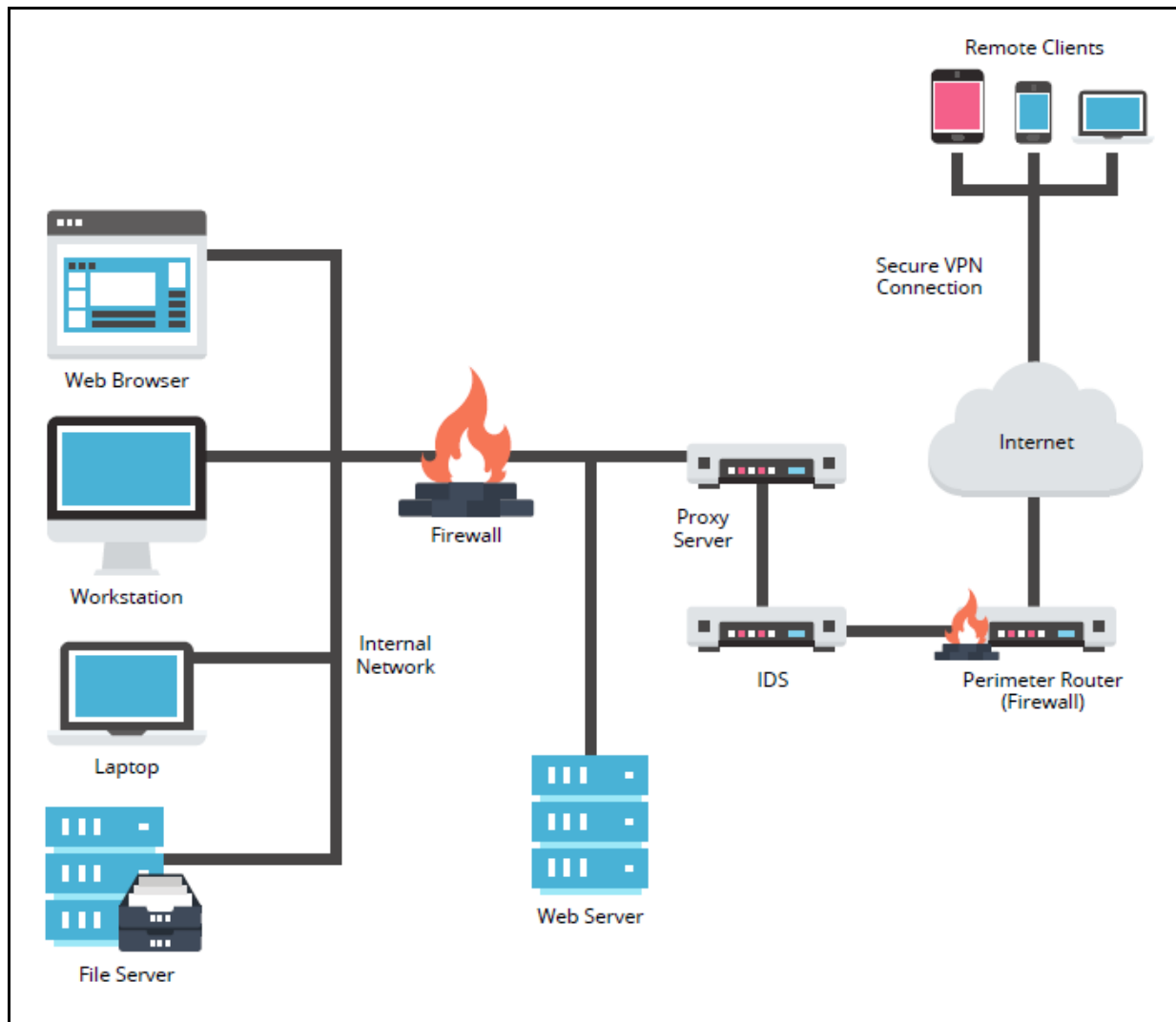
Because network protection devices represent access points into the network, you need to consider their security. It's a good idea to require strong passwords on network devices and to encrypt connectivity between them.

### Controlling Remote Access

**Remote access** is a sticky situation. You need offsite staff to be able to access the internal network. But by granting that access, you may be creating a weak spot in your network's security.

The safest way to allow remote access to an internal network is via a **virtual private network** (VPN), shown in Figure 52. You need a VPN server on your network (or a VPN server service running on an existing server), and you need VPN client software on the remote user's computer.

You can even set up VPN access from a user's mobile phone, recommended in a **BYOD (Bring Your Own Device)** environment.



*Figure 52 A VPN is an encrypted communication tunnel across the internet*

Although a VPN provides safe passage over the internet, there are still dangers to be aware of. If the client (computer or mobile phone) is infected with malware, the malware can spread to the internal network when the client connects. You should require that all clients connecting over a VPN have up-to-date antivirus protection. In addition, by enforcing strong passwords and multi-factor authentication, you reduce the number of ways cybercriminals can attack your system.

## ***Establishing Malware-Free Conditions Throughout a Network***

Updated antivirus software is important to any computing environment. Even with the best antispam and anti-phishing filters running on a mail server, bad stuff can still trickle through. It takes just one email with a malicious attachment and a clicky user to infect an entire network. To be more effective in identifying and controlling viruses, you need a layered approach.

An organization should install security software at the perimeter of a network and on individual workstations, as well as on servers. You want security software at the perimeter because the perimeter network is an entry point from the public internet. Many threats, including virus and malware propagation, originate on the internet.

Perimeter devices, such as firewalls, web servers, and email servers, should all have security software installed. Even with the perimeter protected, you still need antivirus software on workstations. Users may unintentionally introduce viruses directly into the internal network. This may be accomplished with something as simple as a USB drive. Suppose a user took a file home to work on it at night. That home computer is infected by a virus, which spreads to the USB drive. The next day, when the user returns to the office with the USB drive, he plugs it into his computer and unwittingly spreads the virus to it. If his workstation doesn't have up-to-date local antivirus software, his computer may go on to infect other parts of the network.

## ***Implementing Network Access Control and Management***

Many SMEs use network access control mechanisms that allow them to police network entry points. Such systems allow an administrator to configure a ruleset that grants or denies access to the network. These systems often use **health checking** software to evaluate a computer's state before the user can connect to the network. The health check may include validation tasks such as checking for operating system updates and verifying the presence of antivirus software and its update status. If a computer fails the health check, it may be isolated to a specific network segment or denied access altogether.

Say that Karen, a salesperson, arrives at your office for business. While waiting in the lobby, she boots up her laptop. Her laptop detects your company's wireless network, and she successfully connects to it. Unbeknownst to the IT group, Karen's antivirus software is long out of date and a worm is lurking on her computer. The malware now attempts to spread to your company's network.

If your company had a health-check solution in place, it would run a health check before allowing Karen's machine to connect. When the solution identified the worm on her system, it would either isolate her laptop or reject the connection attempt. Because you allowed a connection to occur before first validating the machine's state, you opened your network to exploitation.

## Applying Patches and Security Updates

Because of the enormous amount of source code found in modern-day operating systems, applications, and web browsers, they're susceptible to bugs and security holes. Manufacturers release **patches** and updates whenever security problems are detected or as part of regular updates. For example, Microsoft regularly releases patches on the second Tuesday of every month—called Patch Tuesday—to help keep those systems safe from attackers. Patches for Windows 10 may be released at any time, but are still generally released on patch Tuesday.

Just as you can use tools to ensure antivirus software remains updated, you can also use tools to keep systems updated. Windows is configured by default to receive updates and service packs through the Windows Update feature automatically. By default, Microsoft Windows computers connected to the internet, regularly checks for high-priority updates including security updates, critical updates, and service packs. The service downloads the updates and installs them, as long as the computer is configured for automatic updates. Turning off the automatic updates feature puts a computer at high risk for malware infections and attack.

*On Windows 10, it is possible to delay patch updates by seven days (up to five times) on home computers. For Windows 10 Pro, Enterprise, and Education, you can delay updates for up to 365 days to allow for testing.*

In network environments, you can also use enterprise patch management update products, such as Windows Server Update Services (WSUS) for patch management. WSUS centralizes and automates the management of Windows critical updates. Once you download updates to an WSUS management server, you test them to ensure they don't have unexpected effects on your network or applications. Then you can push them out to workstations and servers at a time when network activity is low.

All operating systems, such as Apple iOS, Linux, and Google Chrome, need patching and have similar mechanisms to Windows and WSUS. All software, firmware, and hardware should be regularly checked to see if patches are available, and if available, applied in a timely manner. Firewalls, IDS/IPS solutions, and other networking devices require occasional updates as well. Essentially, any device or application running on a network should be kept up to date to maintain the tightest security possible.

*Sign up for security and technical alerts to stay on top of the latest threats. You can request Microsoft-related alerts and security bulletins by visiting the Microsoft Technical Security Bulletins website at <https://www.microsoft.com/en-us/msrc/technical-security-notifications>. Another good resource is the USCERT Cyber Security Bulletins website at <https://www.us-cert.gov/ncas/bulletins>.*

\*\*\*

## Chapter 20

### Protecting People and Assets with Security Technology

Network and security administrators must set up procedures and other mechanisms to protect against threats from both outside and inside attackers. These defenses include implementing access controls, defining clear-cut security classifications, separating duties, performing regular security audits, and using security technology where appropriate.

# Chapter 21

## Managing Online Security Issues

In Chapter 7 and Chapter 9, we described a lawsuit filed by construction company Patco against its bank. The details of the lawsuit apply to this chapter as well. Patco alleged that the bank failed to maintain “reasonable security” over its online banking operations. As it happens, cybercrooks stole \$345,000 of Patco’s money because the bank didn’t detect obvious fraudulent funds transfers.

This chapter discusses options for improving endpoint security (workstations, desktops, laptops, and so forth), which is why it appears in Part 3 of this book. Fraudulent funds transfers are an ongoing problem, and SMEs must be aware that online banking (and being connected to the internet in general) carries risks of fraud and theft.

As you work your way through this chapter, you’ll learn about technical measures that can help prevent fraudulent funds transfers. But we see no magic bullets. Funds transfer security is a game of “cops and robbers.” As soon as an attack is discovered and dissected, countermeasures are implemented. But then, a different attack comes along, and the game goes into another round.

In response to a 2009 security blog, well-known security company RSA (now the security division of EMC) posted this memorable statement:

*“Organizations that conduct business online should assume that all of their users’ PCs are compromised in some manner and should prepare their security infrastructures accordingly.”*

Even today, many years later, we can’t think of better security advice for organizations to ponder, then act upon! This is known in computer security circles as an “assume breach” defense strategy. It encourages all organizations to implement defenses as if they were already actively compromised by an attacker or easily could be if an attacker concentrated on compromising them. Sadly, this is true of most organizations, and so, most organizations should implement the appropriate defensive methods and tools. The next few sections describe some of the technologies we recommend to protect endpoint systems. This is meant as a summary of various techniques to help you understand how you can protect your individual and business computer systems.

## *Defense in Depth*

Centuries ago, in medieval times, castles were designed and built to protect people from raiders, pirates, and invasion. Attackers used a variety of tactics in their attempts to conquer these stone fortresses; they could attack on horseback and on foot, use ladders to climb up walls, and even dig tunnels to tunnel under the outer defenses. Because of this, castles used a methodology called defense-in-depth to protect themselves. You can think of it like an onion with several distinct layers around a core – you must go through each layer to get to the center.

Castles were designed to operate in the same manner. The first layer may have consisted of sharpened stakes to protect against raiders on horseback. Behind these, the defenders might dig a trench for infantry to fight against those attackers on foot. A moat was intended to keep the attackers away from the wall, and that was ringed with defenses to protect against people climbing up on ladders. Inside the castle, a group of people acting as a fire brigade would run around putting out any fires from flaming arrows.

Protecting workstations, desktops, laptops – we call these **endpoints** – is done in the same manner. No one defense can protect against everything. Instead, multiple layers of defenses must be used to protect against different threats. If an attack gets through one defense, it might be stopped by another layer, and if it gets through that, there's yet another layer of protection. Let's briefly go through some of those layers in this section. We will look at both commercial and home computer systems.

## *Policies*

For businesses, it's essential to define the policies that guide the security practices of your employees and organization. These policies are often required by various governance standards because setting up and maintaining good security can be complex. These enable everyone to be on the same page and understand what they need to do and how they fit in to keep the organization secure. Policies are intended to be living documents and grow and change as security requirements evolve. A company may begin with a simple policy stating that firewalls and antivirus software are required on each workstation but may grow into more complex requirements as more employees are added.

Consumers generally don't define security policies for their home computer systems and smart phones. Instead, they tend to find applications that fit their security needs and install them. The applications enforce an implicit security policy on their hardware, operating system, and applications.



## Firewalls

To begin with, your system must be protected from access by unauthorized networks and machines. A firewall analyzes network traffic and decides to block or allow communication based on security rules. Firewalls are essential components of good security because they keep many of the bad guys well away from your computer.

For home systems, a firewall is typically installed on your computer and software. Windows 10, for example, comes out-of-the-box with its own firewall system. For good security, this should never be disabled. There are also commercial applications that perform much of the same function. Your cable modem or router generally also contains a firewall to protect against common threats.

Businesses typically install firewalls on the perimeter of their network to protect all their computers at the same time. These firewalls are usually managed by the IT or network department. Even so, the firewall on your computer should remain operational because it adds an additional layer of defense. Intrusion protection systems are an additional layer of defense, typically installed by businesses, and are designed to analyze network traffic to prevent vulnerability exploits.



### **Man-in-the-Middle, Bogus Redirection, and Session Hijacking**

A **man-in-the-middle attack** involves intercepting traffic in both directions for an ongoing connection and then relays all data sent and received between the two parties without the original, authorized parties being none the wiser. The proverbial man in the middle (the attacker) can record, read, or even alter the contents of that traffic. Such attacks are easily foiled with address verification because both sides must interact with the attacker, rather than each other, for this attack to work.

**Bogus redirection** captures traffic addressed to a legitimate site and sends (redirects) it to a different site instead. Some malware does automatic redirection to fool users into thinking they're interacting with a valid and legitimate site rather than a malicious one. Here again, address verification easily foils this type of attack.

**Session hijacking** is an attack method that captures the attributes of a session from one of the parties involved (usually on the client or user end). It then takes over (hijacks) the session from the legitimate user. The attacker keeps the session going and impersonates the user. The user usually blames an internet hiccup for an apparently lost or broken session and simply reconnects through another session. Ongoing connection validation is needed to detect hijacking.

## Patching

Operating systems are extremely complicated and sophisticated collections of software are designed to manage the components of your computer, the network, the screen, printing, and many other things. Bugs are occasionally found in these operating systems and some of these result in security vulnerabilities that allow malicious individuals and applications such as Trojans, viruses, worms, and so forth to gain privileges. These applications can then run amok on your computer causing various types of harm. To keep your system secure, vendors periodically release fixes – known as **patches**. These patches must be installed to prevent hackers and malicious software from getting into your system.

*If you do nothing else to protect your system, you must regularly install security patches in a timely manner. A large majority of security breaches occur as a direct result of an unpatched vulnerability. Patching won't protect you against everything – the other layers discussed in this section are necessary – but it will keep your system safe from a sizable majority of the threats.*

Applications also must be updated or patched regularly. Most modern applications regularly check for updates and patches. Some of them automatically update and others ask your permission first. You must also install these to keep your system safe. Network devices, appliances, hardware, and firmware must also be kept up to date with all applicable security patches as well.

## Password Vaults

If you've been on the internet for any length of time, you've probably wound up with dozens or even hundreds of passwords. Trying to remember all the passwords that you've accumulated can quickly become unmanageable. People solve this in different ways:

- They make all the passwords for all their accounts the same. This is a big mistake, because if hackers break into one account, they gain the passwords for all the accounts. This mistake is magnified if all the accounts use the same username or email address because that makes it even easier for the hackers.
- They write down their passwords on paper near their computer or devices, which hackers can find and use.
- They write their passwords down onto a computer file, which can be captured by hackers or malware.
- They make their passwords simple and easy to guess when possible.

One way around this problem is to use a password manager such as LastPass or 1Password. Some browsers also offer to store passwords in their own internal password vault. While password managers are highly recommended, browser password vaults are not. Many hackers and malware programs routinely steal exploited user's browser stored passwords. But no matter how you store your passwords, they should be unique per website and never shared across sites and services. That's the most important password recommendation there is.

## *Antimalware Applications*

These often go under the name of antivirus applications, but they generally protect against much more than viruses. Today's threats include worms, Trojans, ransomware, viruses, and so forth. To combat these threats, a fully featured antimalware product is required. An antimalware application is essential as part of your layered security plan. However, you can think of it as the last bastion of defense. It's impossible for these applications to protect against everything, but they can help catch many of the attackers that get through your other defenses. There are a multitude of security applications available, and it is beyond the scope of this document to go into them in any detail. Suffice to say that you need to look for a high feature, low performance impact package that protects you from as large a variety of threats as possible.

Microsoft Windows Defender, which comes with Microsoft Windows 10, provides decent protection, although many people like to use other antimalware programs instead. If you don't install or purchase another antimalware product, leave this application turned on. Other products will turn off Microsoft Defender once they're installed so they don't conflict.

## *Anti-Phishing Systems*

Phishing is a known problem, and it always includes certain elements in its many forms. These include:

- ✓ The email origin being different from the reported or claimed origin
- ✓ An appeal for response
- ✓ A link to click (which takes the clicker to a destination of the cybercrook's choosing)

Why is there no technical solution to stop phishing attacks? This question is very interesting. Every major web browser includes anti-phishing elements, all the major security software packages include anti-phishing elements, and numerous technical solutions aim directly at phishing. Yet phishing attacks continue to succeed, despite all these security measures. How can this be?

## Chapter 21

### Managing Online Security Issues

On the banking side, phishing succeeds because many banks don't have or don't use sophisticated fraud-detection and prevention tools. Banking customers don't know this. Thus, most of them fail to use proper safeguards to make up for the bank's lack of fraud detection.

Phishing attacks continue to succeed because people keep falling for phishing emails, tweets, and links on social network pages. As long as users keep clicking those poison links, some of them will lose money. That hasn't stopped software developers and financial institutions from attempting technical solutions to the problem of funds transfer fraud. Let's look at some of these solutions and determine why some have failed and others have succeeded to some degree or other.

### **Anti-Phishing in Web Browsers**

All the major web browsers—Microsoft Internet Explorer (pre-Windows 10), Mozilla Firefox, Google Chrome, Opera, Microsoft Edge (Windows 10), and Apple Safari—include anti-phishing technology. For these browsers, the first line of defense is to check the validity of the digital certificate for websites that users visit. Unfortunately, since the vast majority of malicious websites have a valid digital certificate, most computer security experts consider them poor proof of a website's legitimacy. Most browsers compare all clicked on URLs with a database of previously detected malicious URLs. If a URL you click on is in the database, the browser will warn you and try to prevent you from easily going to the website.

***Blacklisting** is a way to block spam email. If an internet service provider (ISP) blacklists a particular email server, any emails sent from that server to the ISP are automatically discarded. Many email clients offer a built-in method for blacklisting email addresses.*

Email administrators should enable **Sender Policy Framework (SPF)**, **Domain Keys Identified Mail (DKIM)**, and **Domain-Based Message Authentication, Reporting & Conformance (DMARC)**. These are global standards which reduce email domain name forgeries. Enabling them makes it harder for spammers and phishers to make their email appear as if it is coming from another valid domain name when it is not.

Hundreds of anti-phishing software tools, browser add-ins, and URL filtering services are available on today's market. Yet phishing remains real, present, and chronic. Microsoft notes in its discussion of phishing that another key ingredient in avoiding phishing attacks is user education. This area is in urgent need of attention and information. It alone explains why phishing attacks continue to succeed, despite all the money and technology thrown at the problem. Simply put, users keep falling for lures in phishing attacks and keep clicking suspect links! As long as that keeps up, at least some phishing attacks are bound to succeed.

## *Online Reputation*

**Online reputation** is a method normally done by businesses as part of their defense planning, for assessing the credibility of websites, sellers, writers, information providers, and other online players and personalities. Numerous vendors offer online reputation systems. These systems assign numeric values or rankings to assessments. They incorporate ratings from users or buyers, as well as information about spam, malware, and spyware reported for specific sites and addresses. Most internet security software systems provide reputation scores for websites that users seek to visit. This is intended to help steer them away or wave them through to those sites.

## *User Education and Awareness*

A major component of any security policy is the requirement to educate users, so they are aware of security threats and their role in preventing breaches and other issues. No matter what policies and other technical controls you put in place, some amount of malicious content will get to your end users. Users must be educated to understand the concept of phishing and what to do about it, threats from social engineering, and how to respond when they believe there has been a security breach. Without user awareness, security is weakened considerably. On the other hand, a well-thought-out and distributed user awareness program can prevent a multitude of potential breaches in security issues.

\*\*\*

There are many tools that can be used to manage online security issues. Begin by planning a defense in depth, which includes firewalls, patching, password vaults, antimalware and anti-phishing applications, and online reputation tools. User education and awareness must be a high priority since users are one of the primary ways criminals penetrate systems.



# Chapter 22

## Cyber Insurance

It is undeniable that a cyberattack can cause immense harm to your business. Even a small breach can put valuable financial data, customer records, employee information, and even manufacturing facilities at risk. A single breach that results in the loss of consumer information can result in multimillion-dollar lawsuits. In Europe with their GDPR regulations, for example, penalties can range into the billions.

A significant breach can result in any or all the following consequences:

- The operations of your business could slow or even cease entirely.
- Consumers can file lawsuits (including class-action suits) due to the exposure of their personal information.
- Employees and executives can be blackmailed or extorted.
- Government agencies can levy significant fines.
- Internal and external resources will be required to investigate and mitigate any breaches.
- There can be significant damage to the corporate brand.

Adding up the damages from all causes, a breach can result in millions of dollars of losses. In general, the more substantial the breach, the higher the cost. Your company could also undergo intangible damages, such as hits to your reputation and loss of sales. Technology, especially as it relates to the internet, plays a key role in the operation of your business. Most companies today depend on customers and sales from their websites, email, and mobile applications. Every one of these avenues is a target for cybercriminals, whether they are simple hackers, sophisticated cyber gangs, or nation states.

### *What is Cyber Insurance*

Your company can purchase a cyber insurance policy to mitigate the financial risks associated with a breach or other cybersecurity incident. These are often referred to as cyber risk insurance or cyber liability insurance. These policies are based on errors and omissions insurance policies and they started to become popular in 2005. They typically cover direct expenses because of an incident as well as claims by other parties.

## Chapter 22

### Cyber Insurance

Some of the expenses that are covered include:

**Forensics investigation.** Whenever there is a cyber incident, an investigation is performed to determine what happened, how to mitigate the damage, and how to prevent the same thing from happening again. Sometimes these investigations are done by the IT department or an external security company. The police and the FBI may also be involved.

**Losses to the Business.** Typically, anything covered under an errors and omissions policy is also included within the cyber insurance policy. Additional expenses covered include interruption to the business, recovering data, crisis management, and the cost of downtime.

**Notifications.** Many countries and localities require that customers and others be notified of any breaches. Customers whose data was compromised may also require credit monitoring. A cyber insurance policy should take care of these notifications.

**Lawsuits.** Many breaches result in lawsuits by consumers and businesses. A cyber insurance policy should take care of the legal expenses of these suits.

**Extortion.** Many cyber insurance policies cover the cost of extortion.

**Loss or Damage to Reputation.** Cyberattacks and breaches can cause damage to the reputation of your business. Cyber insurance policies help your business recover some of the expenses relating to this damage.

## *Cyber Insurance Statistics*

In 2019, the market for cybersecurity insurance was valued at US\$7.36 billion. It is forecast to reach over US\$27 billion by 2025. The market for cyber insurance is largest in the United States and most vendors that offer these policies are U.S. based.

Large breaches in many major corporations are causing many companies to purchase cyber insurance policies. A few examples of large breaches are listed below: [68]

- ✓ In 2017, a breach at Equifax affected 143 million customers.
- ✓ 153 million records were stolen by hackers from Adobe in 2013.
- ✓ In 2016, Adult Friend Finder suffered from a breach that impacted 412 million accounts.
- ✓ In 2019, Canva suffered from a breach that affected 137 million users.
- ✓ In 2016, LinkedIn was hacked, and 165 million usernames and passwords were stolen.

However, over 27% of U.S. businesses do not have plans to purchase cyber insurance despite the risks [69] and, according to SC Media, only “20% of businesses have invested in cyber insurance.” [70]



## *How is the Price Determined?*

The amount paid for a cyber insurance premium varies from company to company. Small business premiums can range anywhere from US\$1,000 to US\$7,500 for a US\$1,000,000 limit. However, this price depends on your industry, exposure, dollar limits, coverage, and deductibles.

Risk factors that impact insurance costs include: [71]

- ✓ **The limitations, deductibles, and exclusions of your specific policy.**
- ✓ **The security of your infrastructure.** Insurance policy underwriters will audit your controls and procedures to determine how vulnerable your infrastructure is to breach or attack.
- ✓ **Your training procedures.** The risks of a breach or of losses is highly dependent on the training that your users and IT staff obtain. Personnel must be trained to understand the risks and know what to do when an attack occurs. The underwriter of your insurance policy will examine these procedures as part of their pricing model.
- ✓ **Loss history.** Does your company have a history of breaches or losses? This history gives underwriters a picture of exposure and helps them by revealing areas in your organization that are vulnerable to security flaws.
- ✓ **Type of data collected and stores.** Organizations that store credit card data, financial information, or healthcare data tend to be more heavily targeted by cybercriminals. The type of information that the organization collects and stores is used to help determine the risk involved.
- ✓ **Geographic location.** The location of your business and computer infrastructure can increase or decrease your risk.
- ✓ **Regulatory requirements.** Governance policies such as GDPR (for Europe), CCPA (for California), and the Biometric Information Protection Act may increase the accountability of your company when handling sensitive data. These regulations can impose significant fines in the event of breaches or failures to follow procedures.

## *What to Do When There Is an Incident*

Your incident response plan should be thoroughly documented and understood by all the applicable personnel in your organization. Standards such as PCI-DSS (Payment Card Industry Data Security Standard) demand that these plans be maintained and that users are trained periodically so they understand their roles under various scenarios.

An incident response plan prepares your organization on what needs to be done if there is a security breach. This helps the organization make quick decisions. These plans include IT experts, senior management, and subject matter experts from other areas of the business.

## Chapter 22

### Cyber Insurance

In summary, an incident response plan includes the following:

- ✓ Defining who does what during an incident.
- ✓ Defining the roles of the members of the incident response team.
- ✓ Detailing how to contain the damage.
- ✓ Detailing how to eradicate the problem.
- ✓ Documenting how to recover after the problem has been eliminated.
- ✓ Defining the process for documenting lessons learned.

This is an example of an incident and how it is handled when cybersecurity insurance is involved:

1. A breach occurs.
2. The breach is detected.
3. The incident response team is initiated and follows the steps in the incident response plan.
4. Senior management is informed.
5. The cyber insurance company is contacted. They will put an organization in contact with an incident response broker who tells them what they need to do. They act like a general contractor.
6. The incident is resolved according to direction from the incident response broker and your incident plan.

Another good recommendation is to ensure that all communications to any outside agencies, including the cyber insurance company, should be made by a lawyer. This is because those communications become privileged information and they cannot be brought into a court of law easily if ever. This should be stressed in the incident response documentation.

Once an insurance firm is involved, they gain some control over the situation. Since they will be covering claims for losses and damages, they want to make sure that your company responds appropriately and quickly to reduce those damages. This means you may not have the final say about what will be done to handle a cybersecurity incident.

If the organization has or is considering a cyber insurance policy, it's important to create a relationship in advance of an incident with a cyber response broker. Call that broker ahead of time to make introductions, understand all expectations and responsibilities on both sides, and understand the workflow in the event of an incident.

## *Questions to Ask About Cyber Insurance*

Some of the questions you should ask before signing a cyber insurance policy include:

## ***What is covered under a cyber insurance policy?***

Cyber insurance policies mitigate the financial losses that occur from cyber incidents. Some of the expenses include:

- ✓ The direct costs associated with recovering from a breach.
- ✓ The costs of informing customers about an attack or breach.
- ✓ Claims against your own business by third parties.
- ✓ Regulatory fines.
- ✓ Network restoration expenses.
- ✓ Incident response expenses.
- ✓ Business interruption losses.
- ✓ Post-incident remediation expenses.
- ✓ Loss of income.
- ✓ Interruption of the business.
- ✓ Computer forensic expenses.
- ✓ Crisis management expenses.
- ✓ Expenses associated with the PCI forensics investigator.
- ✓ Cyber extortion expenses.
- ✓ Dependent business interruption losses.
- ✓ Notification and identity protection expenses.
- ✓ Cyber terrorism defense expenses.

First party expenses are designed to pay those amounts paid directly by a firm because of a breach. Third-party expenses apply to claims taken against a business by those who have been injured because of their actions or failure to act.

## ***Is the policy an extension to an existing policy or does it stand alone?***

Cyber insurance is available as a standalone policy or may be available as an add-on to an existing liability policy.

## ***Are there any deductibles or coinsurance amounts?***

Review your insurance contract carefully, as these types of policies are relatively new and typically don't have standard coverage language. The terms and coverages of these policies can vary widely. These insurances may have limits, sub limits, and deductibles for both the overall policy and for individual types of coverage. For example, many policies may not cover or may limit claims because of social engineering.

## Chapter 22

### Cyber Insurance

Carefully review the language of the insurance policy as they may appear to broadly cover cyber incidents, but on closer reading, coverage may be found to be narrow and limited. Cyber insurance policies typically contain exclusions, particularly for losses arising from employees who cause a breach due to dishonest, fraudulent, criminal, or malicious conduct as well as intentional violations of the law as well as cyberwarfare (which some cyber insurance firms have used to avoid paying out fines). [72]

### ***Does the policy exclude for criminal or intentional acts?***

Many cyber insurance policies specifically exclude coverages for intentionally criminal or dishonest acts by your own personnel. These include:

- ✓ Breach of contract
- ✓ Theft of trade secrets new
- ✓ Unfair trade practices

An event caused by IT staff members deliberately harming an organization's computer systems would typically not be covered by these insurance policies. For example, coverage may be limited or excluded if an IT employee intentionally destroyed a computer or deleted a database.

### ***What is the liability coverage for third parties?***

Other parties may make claims against a company because of a cyber incident or breach. For example, a company could be sued for negligent acts, errors, and omissions that are the result of a security breach of the infrastructure, or a failure to protect sensitive data. Review the policy carefully to ensure an understanding of the exclusions, deductibles, and limitations of the third-party coverage.

### ***Is social engineering covered?***

Many cyber insurance policies include language to exclude or limit damage or breaches because of social engineering. Since social engineering is responsible for the vast majority of data breaches, you should not allow exclusions or limits involving social engineering. If you do, you are essentially most likely limiting the total protection the policy claims to cover to the lower limits.

### ***Are phishing and spear phishing covered?***

Review the language of the policy carefully to ensure that breaches that happen because of phishing and spear phishing will be covered. Many policies specifically exclude this type of social engineering.

### ***What is the coverage for forensic investigations?***

The expenses incurred because of forensics investigations into the attack or breach are typically covered under cyber insurance policies.

### ***How does the policy handle a breach that is result of negligence rather than maliciousness?***

The coverages for maliciousness and negligence differ from policy to policy. The policy will need to be reviewed to determine how these are covered. Note that many cyber insurance policies exclude coverage if an organization's employees had malicious or criminal intent to damage computer systems.

### ***What are the limits for payouts for each type of coverage?***

All insurance policies include limits and deductibles. Review the policy to understand the limitations imposed upon the organization in the event of various types of breaches.

### ***Does it cover cyberwarfare events?***

Some policies contain exclusions for cyberwarfare events. Review your policy and, if that kind of coverage is important to your organization, make sure it is included.

\*\*\*

Cyber insurance helps organizations mitigate the financial risk associated with cyber incidents. Those risks can be difficult to quantify in advance because the nature of the breach, the level of the threat, and the damage done can vary widely. There's a big difference between an email-based worm that affects a few workstations, cyber espionage of high-level executives, and waking up to find an entire customer database online and available to the public.

Spend the time researching and quantifying the level of risk to the organization and then work with management to determine how much risk is acceptable. This will help determine cyber insurance needs, deductibles, and coverage for the organization.



# Chapter 23

## Fostering Security Awareness

“The internet is the crime scene of the 21st Century.” That quote by Manhattan District Attorney Cyrus Vance, Jr., in an October 2010 *Wall Street Journal* article, sums up the high tech and global state of crime on the internet today.

International cybercrime has gone professional. Web-based crimes are easy to commit, and they rake in billions of dollars annually. The bad guys come up with more and better ways of victimizing us every day. Protections that worked well last year or last month may be useless today, leaving your organization at high risk of data theft and financial loss. SMEs need to be as vigilant as large corporations in keeping the criminals at bay.

This chapter spotlights the most effective means of combating cybercrime: security awareness. You’ll learn what it entails, how it can make or break an SME, and how training can help your organization maintain the upper hand in the fight against cybercrime.

### *What Is Security Awareness?*

The aim of security awareness, or cybersecurity awareness, is to teach people web-based safety techniques and provide a strong shield against cybercrime. Technology provides a lot of protection. Security software monitors emails and web surfing sessions, filtering out a large amount of cybercrud. Network and computer firewalls do a good job keeping outsiders from becoming insiders. Access controls help ensure that only authorized users can use network resources. But no technology protection is perfect.

Cybercriminals come up with new ways to bypass technology guards all the time. In addition, malware evolves rapidly, and phishing gets more sophisticated each month. Only by understanding threats to computers and data while surfing the web (or checking email, instant messaging, or texting) can we learn to avoid becoming victims.

*Crackers and other cybercriminals release 350,000 new malware variants [49] every day and send 14.5 billion spam emails daily [50]. The numbers just keep going up and up.*

## Chapter 23

### Fostering Security Awareness

This book has detailed the cyberthreats you and your employees are likely to encounter. Many things that seem like simple annoyances—spam, email, and pop-up ads in particular—are vehicles for potentially dangerous phishing scams and drive-by downloads. A scammer can steal your organization’s identity, open credit accounts, and run up thousands of dollars of fraudulent purchases. A drive-by download may silently install keylogger software that then captures usernames, passwords, and other private information. Ransomware can hold computers hostage until a fee is paid. By the time you uncover such problems, it’s usually too late: You or your organization will suffer a financial loss, as well as a blow to your reputation if the crime goes public. In severe cases, where the losses are too great or regulatory compliance is breached, organizations fold.

Most SMEs provide some type of sexual harassment training during new employee orientation or annually for all employees. Yet more than 50% of SMEs have no formal policy or security awareness training program in place. Don’t let this happen to your organization. Help your employees recognize phishing emails and scam advertisements. Teach them what to do and what not to do when presented with suspicious messages and links. Security awareness is the essential counter strike against cybercriminals, and it’s the key to avoiding those crimes in almost every case. For the best protection, make security awareness training an essential part of your defense-in-depth strategy and require training for all employees.

#### ***National Cyber Security Awareness Month (NCSAM)***

*October is National Cyber Security Awareness month. Since 2004, this public awareness campaign has encouraged home users, businesses, schools, nonprofits, and government agencies to “protect their computers, children, and data.” Driven in part by the National Cyber Security Alliance (NCSA), the organization wants internet users to understand the impact their online behavior has on web security as a whole and to share the responsibility for making the web a safer place.*

## About Security Awareness Training (SAT)

SAT teaches participants safe surfing and messaging habits. SMEs should encourage SAT for employees to avoid the fallout from cybercrimes. Training helps employees avoid failures and may reduce or eliminate your organization’s liabilities in lawsuits. In addition, employees who have taken SAT generally feel more confident about meeting threats head on. They might also come out of training with a better attitude toward your organization’s security policy—a win-win for everyone.



*Organizations that are regulated—for example, by the Sarbanes-Oxley Act or the Payment Card Industry Data Security Standard (PCI DSS)—require employees to take SAT at least annually to meet compliance requirements. Many states also require state-owned educational institutions to provide SAT for all users.*

It helps to understand more about the history of hacking when you need to defend yourself against cybercriminals. So here is your executive summary:

Early hacking started when guys like Kevin Mitnick became ‘digital delinquents’ and broke into the phone company networks. That was to a large degree to see how far they could get with social engineering and it got them way further than expected. Actual financial damage to hundreds of thousands of businesses started only in the nineties but has moved at rocket speed these last 20 years.

**Generation ONE** – Those were the teenagers writing computer viruses to gain notoriety and to show the world they were able to do it. Most malware creations were relatively harmless, no more than a pain in the neck to a large extent. We call them sneaker-net viruses, as it usually took a person to walk over from one PC to another with a floppy disk to transfer the virus.

**Generation TWO** – These early day ‘sneaker-net’ viruses were followed by a much more malicious type of super-fast spreading Internet worms (we are talking a few minutes) like Sasser and NetSky that started to cause multi-million-dollar losses. These were still more or less created to get notoriety, and teenagers showing off their “elite skills” but hackers start to see their commercial viability.

**Generation THREE** – Here the motive moved from recognition to remuneration. These guys were in it for easy money. This is where botnets came in, thousands of infected PCs owned and controlled by the cybercriminal that used the botnet to send spam, attack websites, identity theft and other nefarious activities. The malware used was more advanced than the code of the ‘pioneers,’ but was still easy to find and easy to disinfect.

**Generation FOUR** – Here is where cybercrime goes professional. The malware starts to hide itself, and they get better organized. They are mostly in eastern European countries and use more mature coders which results in much higher quality malware, which is reflected by the first rootkit flavors showing up. They are going for larger targets where more money can be stolen. This is also the time where traditional mafias muscle into the game, and rackets like extortion of online bookmakers starts to show its ugly face.

**Generation FIVE** – The main event that created the fifth and current generation is that an active underground economy has formed, where stolen goods and illegal services are bought and sold in a ‘professional’ manner, if there is such a thing as honor among thieves. Cybercrime now specializes in different markets (you can call them criminal segments), that when taken all together form the full criminal supply chain. Note that because of this, cybercrime develops at a

## Chapter 23

### Fostering Security Awareness

much faster rate. All the tools are for sale now, and relatively inexperienced criminals can get to work quickly. Some examples of this specialization are:

- ✓ Cybercrime has their own social networks with escrow services
- ✓ Malware can now be licensed and gets tech support
- ✓ You can now rent botnets by the hour, for your own crime spree
- ✓ Pay-for-play malware infection services that quickly create botnets
- ✓ A lively market for zero-day exploits (unknown vulnerabilities)

The problem with this is that it both increases the malware quality, speeds up the criminal ‘supply chain’ and at the same time spreads the risk among these thieves, meaning it gets harder to catch the culprits. We are in this for the long haul, and we need to step up our game, just like the miscreants have done the last 10 years!

### **Benefits of Online SAT**

For many SMEs, training isn’t a core business function. Training is necessary, but the development, management, and delivery of training can pull a manager away from more pressing tasks. In addition, a learning management system (LMS) can be a major upfront investment and requires time and effort to maintain. If you choose online training packages offered by a third party, you don’t need in-house staff and other resources to deliver the training. For a reasonable fee, your employees can attend courses as their schedules allow. Even remote employees, whether in another city or another country, are easily included; all they require is an internet connection.

In addition, online training companies provide course outlines. You know exactly which topics are covered and in what detail, ensuring that all employees receive the same information. Some training companies are willing to brand their courses for your organization with your own logo.

*Some SAT course providers offer onsite training, either at the client’s facility or the training provider’s facility.*

### **Typical SAT Course Topics**

Not every SAT course is the same, so you should compare course outlines carefully before selecting a training partner. Topics typically covered in SAT courses include the following:

- ✓ What cybercrime is and how it continues to thrive
- ✓ How cybercrime reaches its targets through malware, phishing, and social engineering
- ✓ How to protect sensitive information on computers
- ✓ Why security policies, which include password policies and acceptable use policies, are important

- ✓ How failing to adhere to policies affects organizations (for example data theft, financial losses, diminished reputation, legal proceedings) and employees (for example reprimands, terminations)

Now that you know what to expect from SAT courses, let's take a look at KnowBe4's training program.

## KnowBe4 Security Awareness Training

Traditional security awareness training is static, and it's sometimes developed by HR or department managers rather than IT security specialists. Those trainers update courses annually or less often. In today's cybercrime climate, that's not often enough.

KnowBe4 specializes in IT security. KnowBe4's team of security and e-learning specialists provide state-of-the-art courseware (see Figure 53 for one of its many industry awards) that's relevant to individuals, SMEs, and large corporations. Plus, to inoculate your employees against social engineering, KnowBe4 helps customers perform frequent simulated phishing attacks to assist in education and to help with measuring the effectiveness of that education. See <https://www.knowbe4.com/resources/how-to-phish-your-employees/> for more information.



**Figure 53 KnowBe4 delivers comprehensive security awareness training**

KnowBe4's comprehensive security awareness training program helps you and your employees identify and prevent IT security incidents. Its program includes the following:

- ✓ Annual security awareness training for all employees
- ✓ Additional training for end users who are determined to need it

## Chapter 23

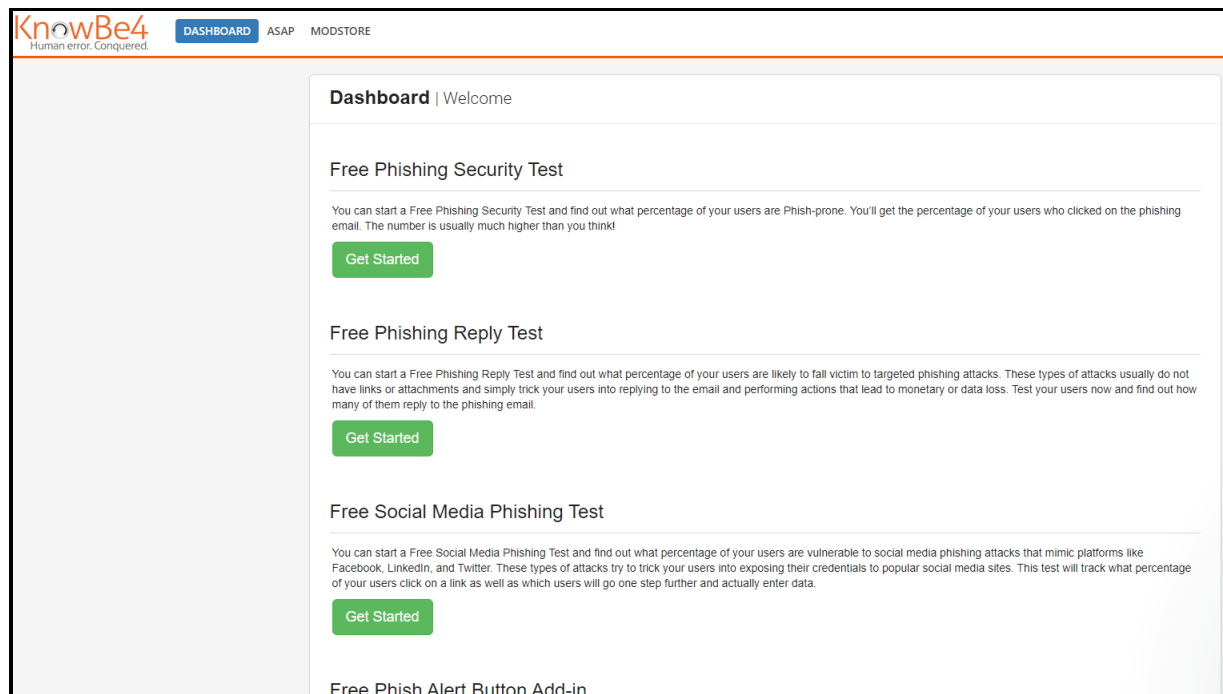
### Fostering Security Awareness

- ✓ On-demand refresher training for all employees
- ✓ Ongoing Phishing Security Tests, which are simulated phishing attacks, so you know the percentage of end users who are Phish-Prone™
- ✓ Training history reports for regulatory compliance

Visit KnowBe4.com for a full list of features.

## Courseware

KnowBe4 has industry leading training and tools with an easy-to-use interface for both users and administrators. KnowBe4 training modules are designed to be effective and engage participants without overwhelming them with information (see Figure 54). A typical module lasts two to 25 minutes. If you need to stop a training session temporarily, the software remembers where you left off. When you return, you can begin from that point.



**Figure 54** *The SAT modules are user friendly and engaging*

Built-in scenarios quiz participants about topics covered in the module. The quizzes are designed to reinforce important cyber safety concepts, and they encourage critical thinking in real-world situations. No special equipment is needed for KnowBe4 training. Participants simply need an internet connection and can use any web browser.

## ***Reporting***

KnowBe4 provides courseware-related reports to managers and project leaders. You'll receive statistics on enrolled employees, their status, completion, and many other parameters.

## ***Pricing***

The following URL lists the current prices for services from KnowBe4:

<https://www.knowbe4.com/pricing-kevin-mitnick-security-awareness-training>

## ***Phish Alert Button***

KnowBe4's Phish Alert Button, which works with Outlook and Gmail gives your users a safe way for users to forward email threats to the security team for analysis and deletes the email from the user's inbox to prevent future exposure. All with just one click!

See <https://www.knowbe4.com/free-phish-alert> for more details.

## ***KnowBe4 Simulated Phishing Security Tests***

KnowBe4 recommends simulated phishing tests to help educate users and to gauge their understanding of the material. Don't let phishers be the only ones testing your end users. KnowBe4 has now helped over 17,000 organizations conduct over 9.1 simulated phishing campaigns against their end users. On average, during the first simulated phishing test, almost 38% of end users will normally click on links or download content within the test emails. After a year of at least monthly education and continuing simulated phishing tests, the Phish-Prone Percentage drops under 5%, as shown graphically in the figure below.

## Visible Proof the KnowBe4 System Works



Employees who fall for an attack will receive an online training reminder as a corrective measure to help them get back on track. Managers and project leaders benefit from the results of the simulated attacks by understanding additional training needs and their organization's overall security compliance. Employees who fail a simulated attack and receive remedial training are 90% less likely to get fooled again in later attacks.

### Consulting Services

KnowBe4 can help you plan and implement a security awareness training program. And you don't need to replace a training program you already have in place. KnowBe4 courses are SCORM (Shareable Content Object Reference Model) compliant. That means we can deliver courseware

for your in-house learning management system, if needed. We also offer competitive upgrade discounts to help you replace your current training program.

### ***How to Contact KnowBe4***

*Visit the KnowBe4.com website to learn more about our programs and services. You can also contact us as follows:*

- ✓ *Send an email to [sales@KnowBe4.com](mailto:sales@KnowBe4.com)*
- ✓ *Call 855-KNOWBE4 (566-9234)*

\*\*\*

Contact KnowBe4 today to find out more about how they can help you improve the security of your systems and infrastructure.





# Appendix A

## Acronyms and Glossary

### List of Acronyms

**ACH:** Automated Clearing House

**ACL:** access control list

**AP:** access point

**AUP:** acceptable use policy

**B2B:** business-to-business

**BBB:** Better Business Bureau

**CEO:** chief executive officer

**CFO:** chief financial officer

**CIA:** confidentiality, integrity, and availability

**CTR:** currency transaction report

**CVN:** card verification number

**DCU:** Dynamic Content Updates

**DDoS:** distributed denial of service

**DoS:** denial of service

**EFT:** electronic funds transfer

**FBI:** Federal Bureau of Investigation

**FDIC:** Federal Deposit Insurance Corporation

**FTC:** Federal Trade Commission

**HR:** human resources

## Appendix A

### Acronyms and Glossary

**HTML:** Hypertext Markup Language

**HUD:** Housing and Urban Development

**IC3:** Internet Crime Complaint Center

**IDS:** intrusion detection system

**IP:** Internet Protocol

**IPS:** intrusion prevention system

**IRS:** Internal Revenue Service

**ISAT:** Internet security awareness training

**ISP:** Internet service provider

**IT:** information technology

**LMS:** learning management system

**NCSAM:** National Cyber Security Awareness Month

**NW3C:** National White-Collar Crime Center

**PBX:** private branch exchange

**PIN:** personal identification number

**PO:** purchase order

**SAR:** suspicious activity report

**SME:** small to medium enterprise

**SMS:** Short Message Service

**SMTP:** Simple Mail Transfer Protocol

**SPF:** Sender Policy Framework

**SSL:** Secure Sockets Layer

**TLS:** Transport Layer Security

**URL:** uniform resource locator

**USB:** universal serial bus

**VoIP:** Voice over Internet Protocol

**VPN:** virtual private network



# Glossary

## access control

A system or technique for allowing or denying access. A door lock is a type of physical access control. Passwords and other types of identification and authorization are also access controls.

## active content

Program code inside one or more objects on a web page. When a web browser accesses a page with active content, the code can be automatically downloaded and executed on the user's PC.

## advance-fee fraud

A type of scam in which a cybercriminal persuades a potential victim to help transfer a substantial amount of money to an account. The victim is offered a commission for facilitating the transaction or multiple transactions. The Nigerian scam, also called the 419 scam, is a prime example of advance-fee fraud.

## application whitelisting

Allowing only known and specifically approved software to execute within an organization's computing systems.

## authentication

The process of identity verification, which can take several forms. A username and password combination is a simple form of authentication.

## Automated Clearing House (ACH)

An electronic network that banks and other financial institutions use to conduct transactions. These transactions use information found on business and consumer checks, normally authorized by that organization or consumer. The transfer might be a single or recurring debit to their account.

## blacklisting

Blacklisting prevents items specifically appearing on a related blacklist from being executed or delivered. For example, an application control program can prevent a blacklisted program from executing or a spam blacklist can prevent email from a blacklisted domain from being delivered.

## bogus redirection

A process that captures traffic addressed to a legitimate website and sends (redirects) it

## Appendix A

### Acronyms and Glossary

to a different website instead. Some malware does automatic redirection to fool users into thinking they're interacting with a valid and legitimate site rather than a malicious one.

botherder

See botmaster.

botmaster

The malicious person in charge of a botnet.

botnet

A network of remotely controlled computers, usually meant for malicious purposes.

Bring your own device

Employees use their own smart phones, tablets and laptops for their work instead of being provided that equipment by the company.

business email compromise

See CEO fraud.

CEO fraud

Criminals target specific organizations and seek to directly infect the computer of the CEO (or another high-level manager). Once malware has been slipped onto their victim's computer, the criminals observe the habits and styles of that CEO, building up a profile of how he or she operates, writes, sounds and acts. After weeks or even months, often when the manager has gone on vacation or a business trip, they send out emails and letters written exactly in the style of the CEO. For example, the CFO might receive an email, seemingly from the CEO, ordering a million dollars to be transferred or paid. Since the order appears to be valid, the CFO probably will perform the fraudulent transfer, and no one will be the wiser until the CEO returns.

challenge-response sequence

A form of identity validation in which the subject wanting to be authenticated is asked to provide one or more answers that only they can successfully answer.

clear text

Unencrypted text stored locally (in memory or on storage) or sent over a network, such as the Internet, that can be read by anyone who captures the transmission.

con man Short for "confidence man," a swindler who gains a person's trust or confidence for the purpose of fraud. Once trust is gained, a fraudster can more easily take the victim's money.

cybercrime

Crime committed using an Internet-connected computer.

cyberheist

Another term for cybercrime.

cyberscamming

Fraud involving computer resources.

dark figure of crime

The amount of crime that remains undiscovered and unknown.

defense in depth

A network protection strategy that uses multiple layers of security.

denial of service (DoS) attack

Overloading a computer with so much traffic or requests that communications to and from that computer are disrupted. Attackers often launch DoS attacks against web servers, preventing anyone else from accessing the associated websites.

digital certificate

A digital stamp or electronic document that attests to the identity of a person or organization. The certificate includes a very secure password issued by a reputable certificate authority, such as VeriSign or Thawte.

distributed denial of service (DDoS) attack

An extension of a DoS attack in which many systems are used to deploy an attack. Using many systems for a DDoS attack allows more disruptive traffic to be sent than can just be sent by a single system, often making it easier to completely disrupt the legitimate service and harder for a victim to recover from the attack.

drive-by download

A transfer of software from a web server to an unsuspecting user's computer. It occurs in the background, with no notification, when a user visits a particular web page. A user need only access the web page to be subject to the download. Such downloads usually include malware when some kind of scam or attack is under way.

Dropper

Malware that lets a hacker download other malware to your computer.

encryption

The process of making clear text unreadable to unauthorized viewers. Before anyone can read encrypted text, it must first be decrypted. By encrypting sensitive data, you can reduce opportunities for criminals to steal sensitive information.

## Appendix A

### Acronyms and Glossary

#### firewalls

Hardware devices or software that restrict the types of traffic that may flow into, through, and out of a security domain.

#### follower

A Twitter user who subscribes to another Twitter user's Tweets. Followers see Tweets from these subscriptions on their own home page.

#### fraud

The criminal act of misleading and misdirecting a victim through trickery.

#### hacktivist

A hacker who is also an activist.

#### harvest

To acquire data illicitly. The data is usually some form of credentials, such as account names or numbers, passwords, and challenge-response sequences. An unauthorized third party—usually, a cyberthief—often uses the information to impersonate the individual or organization whose credentials have been stolen.

#### heuristic detection

A method of malware detection that doesn't depend on knowing the specific signature characteristics of a known type of malware. Heuristic methods look for more generic elements of programs that are indicative of viruses or other malware rather than those types of software that are expected to be found on computers.

#### internet of things

Devices such as smart light bulbs, smart sockets, and smart home alarm systems.

#### keylogger

Malware that records every keypress a user makes on his or her machine into a special file called a keystroke log.

#### malware

Any software that's installed on a device with the intention of executing malicious code and/or causing damage. Typically, the software installs without the owner's permission.

#### malvertising

Using online advertising to infect systems with malware.

#### man-in-the-middle attack

An attack in which data sent and received between two parties in an ongoing connection



is intercepted by an unauthorized third party. The attacker can record, read, or even alter the contents of that traffic.

money mule

A person recruited by a criminal or criminal organization to quickly receive and turn around funds involved in scams. The scams are often related to ACH, credit card, or similar online transactions. The money mule is often unaware of his or her actual role.

multi-factor authentication

A method of validating the identity of a user by using two or more security proofs or methods. For example, a valid username and password combination along with a fingerprint scan is a form of multi-factor authentication.

Nigerian scam

A fraud often perpetrated via email in which a scamster promises financial gain in return for funds advanced. The scam began in the 1980s, at the decline of a once oil-based Nigerian economy. Dozens of variations now exist throughout different countries. Also called the 419 scam.

Number Harvesting

A VoIP attack in which an attacker monitors incoming and outgoing calls on a VoIP system they have broken into.

one-factor authentication

A method of validating the identity of a user by a single credential or set of credentials. A valid username and password combination is a form of one-factor authentication.

online reputation

A ranking system for assessing the credibility of websites, sellers, writers, information providers, and other online players and personalities.

packet analyzer

See sniffer.

password phrase techniques

Methods of producing strong passwords. One technique involves creative transformations for a sentence so that, for example, "I never eat rye bread" becomes iN3V3RtaeWRYdearb.

phishing

Email fraud that uses various techniques to persuade someone to divulge sensitive or confidential information, such as credit card or bank information. Phishing is a kind of social engineering attack. Note it can also be accomplished using voice calls and SMS text messaging.

## Appendix A

### Acronyms and Glossary

#### phone number harvesting

Gathering cellphone or voice over Internet Protocol (VoIP) numbers for advertising purposes, to make unauthorized calls, or for other deceptive purposes.

#### phreaking

A form of fraud that involves directly hacking telecommunications systems.

#### principle of least privilege

Giving users the least amount of access required for them to complete their jobs.

#### protocol analyzer

See sniffer.

#### proxy server

A computer or an application that acts as an intermediary for requests between a client workstation and a server. A common use of proxy servers is to cache web pages or files that are frequently requested. Providing the cached pages reduces network traffic.

#### Public Shaming

Ransomware hackers will publicly reveal the victims of their ransomware programs, along with what was stolen (i.e. confidential data and logon credentials) so they cannot hide the exploitation from their customers or regulators.

#### ransomware

Malware which holds a computer hostage by blocking access, encrypting files, and/or threatening to reveal sensitive data until a ransom is paid.

#### Ransomware as a Service

Provide ransomware to hackers as an online service, complete with constant updates, avoidance of antivirus protection and control from a centralized console.

#### rogueware

Spyware or other malware that often masquerades as antivirus software or other disk utilities such as disk defraggers. Users respond to bogus virus discovery pop-up ads or repair offers to help them get rid of viruses they don't really have. Instead, malware is installed on their machines.

#### safe computing

The application of safeguards and precautions that protect you from becoming a victim of computer crimes, especially cybercrime.

#### safe surfing

A user's cautious behavior when browsing the Web.

Security awareness training

The training to educate employees to be aware of security risks and how they can maintain security. Generally, users receive information about best security practices, what to do if they encounter a security problem, and who to contact for security threats.

security policy

A written document that states how an organization plans to protect its physical assets and information.

separation of duties

Ensures that one person can't solely handle critical tasks. Requires two or more people to collude to do something in order to make rogue actions more unlikely to occur.

session hijacking

An attack method that captures the attributes of a website session from one of the parties involved (usually on the client or user end). It then takes over (hijacks) the session from the legitimate user. The attacker keeps the session going and impersonates the user.

Simple Mail Transfer Protocol (SMTP)

An Internet standard used for sending and receiving email.

smishing

Phishing conducted via Short Message Service (SMS), a telephone-based text messaging service. A smishing text, for example, attempts to entice a victim into revealing personal information.

sniffer

A network tool that captures data transmitted across a cable or wireless connection and lets the user analyze the data to determine its payload. Also referred to as a packet analyzer or protocol analyzer.

social engineering

The act of tricking people into divulging information or performing an action that they shouldn't with an unauthorized third party. Also, the act of gaining sensitive information by deception.

social media

The platforms, or channels, used for social networking. Examples of communication channels are Facebook, Twitter, blogs, and YouTube.

social networking

Actively engaging in online conversations with other people or groups of people. Communication is multidirectional because social networking is all about connecting, collaborating, and sharing information freely.

## Appendix A

### Acronyms and Glossary

#### spam

Unsolicited, junk email usually sent in massive broadcasts.

#### spear phishing

A type of phishing attack that is aimed at a specific organization or company. Spear phishing messages may appear to originate from a large or well-known company or website, a coworker, or an internal manager.

#### spoofing

Making it appear an email, transaction, website, or any other object appears to have originated from someone other than the actual source.

#### steganography

The art or practice of hiding digital information within content, such as messages, images, sounds, etc.

#### tabnabbing

Using browser tabs to impersonate legitimate websites and create fake login pages that trick victims into revealing private information. Tabnabbing works when you have two or more tabs open in a web browser. When a tab is left unattended for several minutes, a tabnabber can redirect the site in the unattended tab to a different, malicious login site. Modern browsers such as Firefox, Chrome, Edge, and Safari prevent tabnabbing, but this can happen on older ones like Internet Explorer.

#### tailgating

A method used by social engineers to gain access to a building or other protected area. A tailgater waits for an authorized user to open and pass through a secure entry and then follows right behind.

#### Trojan (or Trojan horse)

A trojan is a program which hides its true malicious intent by masquerading as another type of program in order to get an unsuspecting user to execute it. Once executed it can do anything the software or hardware is capable of. Common types of trojans are ransomware programs, credential theft, and key loggers.

#### typosquatting

Purchasing a web domain that is a character or two different from a legitimate and well-known social or company website. When a person mistypes the web address, a website appears that looks very much like the intended site. Typosquatting is usually done for fraudulent purposes. Also called URL hijacking.

#### URL shortening

A method of reducing the size and complexity of web URLs, mainly for ease of use or to save space. These are often used in Twitter to save character space. However, URL

shortening also disguises a website's real domain name, and hinders detection of known malicious sites or destinations.

vishing

A phishing attack conducted by telephone, usually targeting voice over IP (VoIP) users, such as Skype users.

voicemail overloading

Spamming over Internet telephony. Much like getting spam email, a voice over Internet Protocol (VoIP) user can get junk voicemails. Spammers simply send a voicemail message to thousands of IP addresses at a time.

whaling

Phishing attacks that target high-ranking executives at major organizations or other highly visible public figures.

zombie

Computer or device under the control of a botmaster.



# Appendix B

## Resources

This appendix lists several cybercrime- and security-related resources aimed at small to medium enterprises (SMEs), many of which are included in this book.

### Banking Security

#### Bank Info Security

[www.bankinfosecurity.com/](http://www.bankinfosecurity.com/)

This news site is chockfull of articles related to financial fraud, data breaches, and security compliance. Sign up for the e-newsletter or register with the site to get breaking news alerts and cyber advisories delivered to your inbox.

### Credit Card Security

#### Payment Card Industry (PCI) Security Standards Council

[www.pcisecuritystandards.org/smb](http://www.pcisecuritystandards.org/smb)

The PCI Security Standards Council site provides detailed guidance on cardholder data security. Any organization that accepts credit or debit cards as payment for goods or services should already be highly familiar with this website.

#### VISA Security Sense

[www.VisaSecuritySense.com](http://www.VisaSecuritySense.com)

Aimed at consumers and organizations, this site provides tips for protecting cardholder security, preventing fraud, and more. The Fraud News and For Retailers sections are good resources for SMEs.

## General Scam/Fraud Information and Security

### Better Business Bureau

[www.bbb.org](http://www.bbb.org)

The Resource Library at [www.bbb.org/us/Business-Resources/](http://www.bbb.org/us/Business-Resources/) includes an Alerts link that describes recent scams and marketplace issues. You may also browse the Data Security – Made Simpler pages at [www.bbb.org/data-security/](http://www.bbb.org/data-security/) for general security information, or download and read the Security & Privacy – Made Simpler guide from [www.bbb.org/us/corporate-engagement/security/](http://www.bbb.org/us/corporate-engagement/security/).

### Computer Crime Research Center

[www.crime-research.org/](http://www.crime-research.org/)

A collection of news feeds, articles, and forums based on computer crime, Internet fraud, and cyberterrorism. The site is run by a nonprofit, non-governmental, scientific research organization.

### Consumer Fraud Reporting (CFR)

[www.crime-research.org/](http://www.crime-research.org/)

A collection of news feeds, articles, and forums based on computer crime, Internet fraud, and cyberterrorism. The site is run by a nonprofit, non-governmental, scientific research organization.

### Home Computer Safety

[www.leavemycomputeralone.com](http://www.leavemycomputeralone.com)

A collection of articles about how to keep your home computer safe from malware.

### Microsoft Technical Security Notifications

<http://technet.microsoft.com/en-us/security/dd252948.aspx>

You can sign up for Microsoft-related alerts and security bulletins at this website.

### SecurityWeek

[www.securityweek.com](http://www.securityweek.com)

This well-known and respected weekly magazine is a first-stop for many SMEs looking for the latest business security news.



### **StaySafeOnline.org**

<http://staysafeonline.org>

The For-Business section includes tips for protecting your organization, employees, and customers from cyber-related crime.

## **Government Agencies**

### **Federal Bureau of Investigation (FBI) Cyber Crime**

[www.fbi.gov/about-us/investigate/cyber/cyber](http://www.fbi.gov/about-us/investigate/cyber/cyber)

### **Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3)**

<http://www.ic3.gov/>

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant.

### **Federal Deposit Insurance Corporation (FDIC)**

[www.fdic.gov](http://www.fdic.gov)

The FDIC website provides information on banking industry regulations, bank closures, statistics, and analyses. Special alerts (SAs) notify the public of banking-related scams and issues. You can sign up by email or RSS to get SAs sent to you, or just visit the Special Alerts section of the website periodically.

### **Federal Trade Commission (FTC)**

<http://ftc.gov/>

The FTC provides information to help consumers spot and avoid fraudulent practices in the marketplace. The Privacy & Security section (<http://www.consumer.ftc.gov/topics/privacy-identity>) offers tips that are useful to SMEs and their employees, too.

The FTC Bureau of Consumer Protection Business Center at <http://business.ftc.gov/> offers a plethora of information for SMEs related to fraud protection, privacy issues, and complying with regulations.

### **Internet Crime Complaint Center (IC3)**

[www.ic3.gov/default.aspx](http://www.ic3.gov/default.aspx)

## Appendix B

### Resources

The IC3 is a joint partnership between the FBI and the National White-Collar Crime Center (NW3C). The organization receives cybercrime complaints and reports statistics, acting as a central referral system for law enforcement and regulatory agencies. The IC3 also provides the annual Internet Crime Report as a free download.

#### **OnGuardOnline**

[www.onguardonline.gov](http://www.onguardonline.gov)

This website provides great antifraud prevention tips. Its File a Complaint section lets you get information on many different scams, and gives clear information on where to report Internet-related frauds, scams, and suspicious activity.

#### **United States Computer Emergency Readiness Team (US-CERT)**

[www.us-cert.gov](http://www.us-cert.gov)

The US-CERT website is the go-to place for top-notch information on business security. To stay on top of the latest threats, visit [www.us-cert.gov/cas/bulletins/](http://www.us-cert.gov/cas/bulletins/) to sign up to receive weekly Cyber Security Bulletins, delivered to your inbox.

## Protection Software and Utilities

#### **Microsoft Safety & Security**

[https://www.microsoft.com/security/pc-security/password-checker.aspx?WT.mc\\_id=Site\\_Link](https://www.microsoft.com/security/pc-security/password-checker.aspx?WT.mc_id=Site_Link)

This password-checker website lets you test the strength of a password.

Security Policy Templates

#### **SANS Information Security Policy Templates**

[www.sans.org/security-resources/policies/](http://www.sans.org/security-resources/policies/)

You can find a wealth of sample security policy templates at this website. The templates are free to use and can greatly speed up security policy implementation at your organization.

## Who to Contact/Where to Complain

If you've received a phishing email, forward it to [spam@uce.gov](mailto:spam@uce.gov). You should also forward it to the organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

If you receive suspicious email that includes the name and/or logo of the FDIC, the Patriot Act, or another federal agency and believe it's a scam, report it to the FDIC. You can forward the email to [alert@fdic.gov](mailto:alert@fdic.gov) or call the FDIC directly at 877-ASK-FDIC.

To report problems with online transactions (between buyer and seller) or office supply scams, contact:

- The FTC, <https://www.ftccomplaintassistant.gov/>
- Your state attorney general, [www.naag.org](http://www.naag.org)
- Your county or state consumer protection agency
- The Better Business Bureau, <http://www.bbb.org/>



# Appendix C

## References

- [1] "Internet Usage by Language: Top 10 Languages," [Online]. Available: <http://www.internetworldstats.com/stats7.htm>.
- [2] "FBI's IC3 2014 Internet Crime Report," 2015. [Online]. Available: [https://www.fbi.gov/news/news\\_blog/2014-ic3-annual-report](https://www.fbi.gov/news/news_blog/2014-ic3-annual-report).
- [3] D. Walker, "Free Trojan kit includes a backdoor that spies on hackers," 1 September 2017. [Online]. Available: <https://www.itpro.co.uk/security/29376/free-trojan-kit-includes-a-backdoor-that-spies-on-hackers>.
- [4] "Behind enemy lines in our war against account hijackers," 6 11 2014. [Online]. Available: <https://googleonlinesecurity.blogspot.com/2014/11/behind-enemy-lines-in-our-war-against.html>.
- [5] "Liability of consumer for unauthorized transfers," [Online]. Available: <https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1005/6/>.
- [6] D. W. Maure, The Big Con, 1999.
- [7] "Chain Letters," [Online]. Available: <https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/sweepstakesfraud/ChainLetters.aspx>.
- [8] "The Challenge of Health Care Fraud," [Online]. Available: <https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx>.
- [9] H. Munir, "Largest Medicare Fraud Takedown In History Occurs," 27 January 2020. [Online]. Available: <https://healthunits.com/news/largest-medicare-fraud-takedown-history/>.
- [10] S. Greenspan, Annals of Gullibility: Why We Get Duped and How to Avoid It, Praeger, 2008.
- [11] "Social Engineering," [Online]. Available: <https://www.techopedia.com/definition/4115/social-engineering>.

## Appendix C

### References

- [12] "Social engineering," [Online]. Available: [http://www.webopedia.com/TERM/S/social\\_engineering.html](http://www.webopedia.com/TERM/S/social_engineering.html).
- [13] "Social engineering (security)," [Online]. Available: [https://en.wikipedia.org/wiki/Social\\_engineering\\_%28security%29](https://en.wikipedia.org/wiki/Social_engineering_%28security%29).
- [14] Wikipedia, "Stressor," [Online]. Available: <https://en.wikipedia.org/wiki/Stressor>.
- [15] "Multi-Stage Phishing Attacks Launch Local Files to Evade Existing Security," 6 May 2020. [Online]. Available: <https://www.slashnext.com/blog/multi-stage-phishing-attacks-launch-local-files-to-evade-existing-security/>.
- [16] "Confirmed Transactions Per Day," [Online]. Available: <https://www.blockchain.com/charts/n-transactions>.
- [17] M. Sonnenshein, "Cryptocurrency," 5 May 2020. [Online]. Available: <https://www.investopedia.com/terms/c/cryptocurrency.asp>.
- [18] "What Are Spear Phishing Attacks," 22 July 2018. [Online]. Available: <https://latesthackingnews.com/2018/07/22/what-are-spear-phishing-attacks/>.
- [19] J. Markoff, "Larger Prey Are Targets of Phishing," 16 April 2008. [Online]. Available: [http://www.nytimes.com/2008/04/16/technology/16whale.html?\\_r=0](http://www.nytimes.com/2008/04/16/technology/16whale.html?_r=0).
- [20] T. Hooker, "Spear phishing and whaling attacks on the rise!," 4 September 2015. [Online]. Available: <https://smxemail.com/spear-phishing-and-whaling-attacks-on-the-rise.html>.
- [21] P. Muncaster, "Dutch Film Boss Sacked After €19m BEC Loss," 14 November 2018. [Online]. Available: <https://www.infosecurity-magazine.com/news/dutch-film-boss-sacked-after-19m/>.
- [22] E. Phil, "CEO Sacked After \$56 Million Whaling Attack," 31 May 2016. [Online]. Available: <https://www.infosecurity-magazine.com/news/ceo-sacked-after-56-million/>.
- [23] J. Rey, "Business Cyber Attacks Top 4,000 Per Day: Your Guide to Ransomware," 30 November 2016. [Online]. Available: <https://www.entrepreneur.com/article/284754>.
- [24] B. Sobers, "110 Must-Know Cybersecurity Statistics for 2020," 15 April 2020. [Online]. Available: <https://www.varonis.com/blog/cybersecurity-statistics/>.
- [25] "Astonishing Cybercrime Statistics in 2019... So Far!," 2019. [Online]. Available: <https://cybriant.com/2019-cybercrime-statistics/>.

- [26] B. Stack, "Here's How Much Your Personal Information Is Selling for on the Dark Web," 6 December 2017. [Online]. Available: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.
- [27] Symantec, "Internet Security Threat Report Feb 2019," February 2019. [Online]. Available: <https://docs.broadcom.com/doc/istr-24-2019-en>.
- [28] "Patco Construction Company, Inc v. People's United Bank d/b/a Ocean Bank," 3 July 2020. [Online]. Available: <http://krebsonsecurity.com/wp-content/uploads/2012/07/First-Circuit-Order-070312.pdf>.
- [29] "Patco Construction Company, Inc v. People's United Bank d/b/a Ocean Bank," 3 July 2012. [Online]. Available: <http://krebsonsecurity.com/wp-content/uploads/2012/07/First-Circuit-Order-070312.pdf>.
- [30] Verizon, "2020 Data Breach Investigations Report," 2020. [Online]. Available: <https://enterprise.verizon.com/resources/reports/dbir/>.
- [31] Chubb, "Chubb's SME Survey ("Too Small to Fail?") Reveals Significant Perception Gap in Cyber Awareness and Preparedness in Singapore, Hong Kong SAR and Australia," 13 February 2019. [Online]. Available: <http://chubb.mediaroom.com/news-releases?item=125175>.
- [32] D. Palmer, "Mobile malware attacks are booming in 2019: These are the most common threats," 25 July 2019. [Online]. Available: <https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/>.
- [33] B. Small, "Scammers offer facemasks but don't deliver," 30 April 2020. [Online]. Available: <https://www.consumer.ftc.gov/blog/2020/04/scammers-offer-facemasks-dont-deliver>.
- [34] Trustwave, "Post-Soviet Bank Heists: A Hybrid Cybercrime Study," 10 October 2017. [Online]. Available: <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/post-soviet-bank-heists-a-hybrid-cybercrime-study/>.
- [35] M. J. Schwartz, "Report: Malware-Wielding Hackers Hit Taiwanese Bank," 9 October 2017. [Online]. Available: <https://www.bankinfosecurity.com/report-malware-wielding-hackers-hit-taiwanese-bank-a-10368>.
- [36] The London Post, "Hackers steal £650 million in world's biggest bank raid," 16 February 2015. [Online]. Available: <https://thelondonpost.net/hackers-steal-650-million-in-worlds-biggest-bank-raid/>.

## Appendix C

### References

- [37] K. Zetter, "Four Indicted in Massive JP Morgan Chase Hack," 11 November 2015. [Online]. Available: <https://www.wired.com/2015/11/four-indicted-in-massive-jp-morgan-chase-hack/>.
- [38] Keeper Security Inc., "2019 Global State of Cybersecurity in Small and Medium-Sized Businesses," October 2019. [Online]. Available: [https://www.keeper.io/hubfs/2019%20Keeper%20Report\\_Final%20\(1\).pdf](https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf).
- [39] J. Buntinx, "Top 4 Largest Botnets to Date," 7 January 2017. [Online]. Available: <https://themerkle.com/top-4-largest-botnets-to-date/>.
- [40] K. Thomas, "Nine bad botnets and the damage they did," 25 February 2015. [Online]. Available: <https://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage/>.
- [41] JP Morgan, "Payments Fraud and Control Survey Report," 2020. [Online]. Available: <https://www.jpmorgan.com/content/dam/jpm/commercial-banking/documents/fraud-protection/afp-fraud-survey-2020-report-highlights.pdf>.
- [42] L. Thomas, "Holiday sales climb 4.1%, retail industry trade group says, on the higher end of estimates," 10 January 2020. [Online]. Available: <https://www.cnn.com/2020/01/16/the-national-retail-federation-nrf-releases-2019-holiday-sales.html>.
- [43] F. McKenna, "The Top Fraud Losses and Trends For 2019," 24 October 2019. [Online]. Available: <https://frankonfraud.com/fraud-trends/the-top-fraud-losses-for-2019-by-fraud-type/>.
- [44] "The economics of unused gift cards," 4 January 2020. [Online]. Available: <https://thehustle.co/what-happens-to-unused-gift-cards/>.
- [45] "Gift Cards Market Outlook - 2027," [Online]. Available: <https://www.alliedmarketresearch.com/gift-cards-market>.
- [46] M. Cerullo, "Consumers waste up to \$3 billion in unspent gift cards a year," 3 January 2020. [Online]. Available: <https://www.cbsnews.com/news/unused-gift-cards-add-up-to-3-billion-annually/>.
- [47] "Facebook by the Numbers: Stats, Demographics & Fun Facts," 22 April 2020. [Online]. Available: <https://www.omnicoreagency.com/facebook-statistics/>.
- [48] T. Ball, "The History of Ransomware," 23 February 2018. [Online]. Available: <https://www.cbronline.com/news/the-history-of-ransomware>.



- [49] M. Yates, "The Cost of Ransomware," 9 May 2016. [Online]. Available: <https://www.avg.com/en/signal/the-cost-of-ransomware>.
- [50] P. Higgins, "The Wannacry Cyber Attack: A Case Analysis," 7 November 2018. [Online]. Available: <https://www.corporateresponsibilitynetwork.com/wannacry-cyber-attack/>.
- [51] OODA Analyst, "Allied Universal Breached by Maze Ransomware, Stolen Data Leaked," November 2019. [Online]. Available: <https://www.oodaloop.com/briefs/2019/11/22/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/>.
- [52] S. N. a. G. Corfield, "Ransomware scumbags leak Boeing, Lockheed Martin, SpaceX documents after contractor refuses to pay," 10 April 2020. [Online]. Available: [https://www.theregister.com/2020/04/10/lockheed\\_martin\\_spacex\\_ransomware\\_leak/](https://www.theregister.com/2020/04/10/lockheed_martin_spacex_ransomware_leak/).
- [53] S. Sjouwerman, "[Heads Up] The REvil Ransomware Gang Is Now \*Auctioning Off\* Their Victim Data," 2 June 2020. [Online]. Available: <https://blog.knowbe4.com/heads-up-the-revil-ransomware-gang-is-now-auctioning-off-their-victim-data>.
- [54] "The Nation State Actor," [Online]. Available: <https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor>.
- [55] Wikipedia, "Convention on Cybercrime," [Online]. Available: [https://en.wikipedia.org/wiki/Convention\\_on\\_Cybercrime](https://en.wikipedia.org/wiki/Convention_on_Cybercrime).
- [56] B. Brake, "The Legal Problems with Cyber War Are Much Bigger Than You Think," 5 August 2015. [Online]. Available: <https://www.defenseone.com/ideas/2015/08/legal-problems-cyber-war-are-much-bigger-you-think/118883/>.
- [57] Wikia.Org, "Cyberwarfare in the United States," [Online]. Available: [https://military.wikia.org/wiki/Cyberwarfare\\_in\\_the\\_United\\_States](https://military.wikia.org/wiki/Cyberwarfare_in_the_United_States).
- [58] Wikipedia, "Sony Pictures hack," [Online]. Available: [https://en.wikipedia.org/wiki/Sony\\_Pictures\\_hack](https://en.wikipedia.org/wiki/Sony_Pictures_hack).
- [59] A. Hope, "DHS Warns of a Persistent Cyber Threat Targeting Critical Infrastructure in the U.S.," 3 August 2020. [Online]. Available: <https://www.cpomagazine.com/cyber-security/dhs-warns-of-a-persistent-cyber-threat-targeting-critical-infrastructure-in-the-u-s/>.

## Appendix C

### References

- [60] B. Barrett, "How China's Elite Hackers Stole the World's Most Valuable Secrets," 20 December 2018. [Online]. Available: <https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/>.
- [61] A. Greenberg, "OPM Now Admits 5.6m Feds' Fingerprints Were Stolen By Hackers," 23 September 2015. [Online]. Available: <https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/>.
- [62] J. Fruhlinger, "What is Stuxnet, who created it and how does it work?," 27 August 2017. [Online]. Available: <https://www.csoononline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html>.
- [63] "Statement by NCSC Director William Evanina: 100 Days Until Election 2020," 24 July 2020. [Online]. Available: <https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020>.
- [64] K. Sheridan, "Rise of Nation State Threats: How Can Businesses Respond?," 19 June 2017. [Online]. Available: <https://www.darkreading.com/attacks-breaches/rise-of-nation-state-threats-how-can-businesses-respond/d/d-id/1329171>.
- [65] "Phishing Activity Trends Report 4th Quarter 2019," [Online]. Available: [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q4\\_2019.pdf](https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf).
- [66] D. Swinhoe, "The 15 biggest data breaches of the 21st century," 17 April 2020. [Online]. Available: <https://www.csoononline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.
- [67] "Cyber Insurance Stats," [Online]. Available: <https://cyberinsureone.com/stats/>.
- [68] D. Taylor, "Cyber Insurance Trends 2020," 6 February 2020. [Online]. Available: <https://foundersshield.com/cyber-insurance-trends-2020/>.
- [69] D. Taylor, "Cyber Insurance Trends 2020," 6 February 2020. [Online]. Available: <https://foundersshield.com/cyber-insurance-trends-2020/>.
- [70] T. Beekley, "The Value and Limits of Cyber Insurance," 23 April 2018. [Online]. Available: <https://er.educause.edu/articles/2018/4/the-value-and-limits-of-cyber-insurance>.
- [71] A. Bera, "38 Interesting Malware Statistics," 2 April 2019. [Online]. Available: <https://safeatlast.co/blog/malware-statistics/>.

- [72] Spam Laws, "Spam Statistics and Facts," 2020. [Online]. Available: <https://spamlaws.com/spam-stats.html>.
- [73] "FBI's IC3 2019 Internet Crime Report," 2015. [Online]. Available: [https://pdf.ic3.gov/2019\\_IC3Report.pdf](https://pdf.ic3.gov/2019_IC3Report.pdf).
- [74] "Online Banking Fraud: Who is Liable," [Online]. Available: <https://www.bncbank.com/files/OnlineBankingFraud.pdf>.
- [75] G. Egan, "2019 State of the Phish: Attack Rates Rise, Account Compromise Soars," 24 January 2019. [Online]. Available: <https://www.proofpoint.com/us/security-awareness/post/2019-state-phish-attack-rates-rise-account-compromise-soars>.
- [76] S. Fadilpašić, "Welcome to the era of Ransomware 2.0," 12 February 2020. [Online]. Available: <https://www.itproportal.com/news/welcome-to-the-era-of-ransomware-20/>.
- [77] T. NewsLagoon, "Law firm hackers shift ransom target from Donald Trump to Madonna," 18 May 2020. [Online]. Available: <https://newslagoon.com/entertainment/law-firm-hackers-shift-ransom-target-from-donald-trump-to-madonna/101441/>.
- [78] Sophos, "The State of Ransomware 2020," 2020. [Online]. Available: <http://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>.



# Index

419 scam, **20**, 92  
Acceptable use policies, 202  
**Acceptable use policy**, 200, 218  
Access control mechanisms, 220  
Access controls, **193**  
Access logs, 206  
Access sensitivity, 213  
Account number, 129  
ACH. See Automated Clearing House  
ACH fraud, 107  
ACH network, 129  
ACH scams, 13, 131, 137  
ACH transfer, 129  
**ACH transfers**  
    **Fraud**, 9  
**Active content**, 33  
ActiveX controls, 33  
**Administrator**, 210  
Adobe Flash, 34, **47**  
Advanced-Fee Scam, **20**  
Advance-fee fraud, **92**  
**Advertisements**  
    **Popup**, 9  
Adware, 195  
AIDS Cop trojan, 157  
Airports, 194  
Annual losses, **82**  
Antifraud, 119  
Anti-malware, 227  
Anti-phishing, 227  
Anti-phishing filters, 220  
Antisпам, 220  
Antispyware, 195  
Antivirus, 195, 227  
Antivirus software, 220

**Application whitelisting**, **110**  
Archiveus Trojan, 157  
Asymmetric encryption, 157  
**Auction Your data**, 165  
**Authentication**, **58**, 61, 67, 187  
Automated Clearing House, **7**, 129  
Backups  
    Ransomware, 160  
Bailout scam, 122  
Bait-and-switch scam, 122  
**Bank account**  
    **Scams**, 11  
Bank scam, 103  
Banking authentication, 107  
Banner advertisements, 35  
Better Business Bureau, 123  
Bitcoin, 36  
    Ransomware, 157, 158  
**Blacklisting**, **228**  
Blogs, 154  
Bogus Account Credit Scams, 145  
Bogus redirection, **225**  
Botherder, **112**  
Botmaster, **112**  
Botnet, **68**, 111, 114  
Brick and Mortar Store Scams, 142  
Bring Your Own Device, **36**, 219  
Browser extensions, 34  
Business Email Compromise (BEC), **79**  
Business Page, 155

**BYOD**, 219  
CEO Fraud, **35**, **79**  
Chain letter fraud, 20  
Challenge-response sequences, **9**  
Chip and Pin Cards, 120  
Clear text, **192**  
Coffee shops, 194  
Communications, 168  
Computer crime, **4**  
Con man, **17**  
Confidence man, 18  
Consulting services, 246  
Coupons, 155  
COVID-19 pandemic, 122  
Craigslist, 125  
Credential hygiene, 167  
Credibility, 90  
Credit card fraud, 112  
Credit card scams, 111  
Credit cards  
    Legal Protection, 14  
Critical updates, 221  
Cryptocurrencies, 36  
Cryptolocker, 158  
CryptopWall v3, 158  
Cyber insurance policy, 231  
Cyber insurance premium, 233  
Cyber liability insurance, 231  
Cyber risk insurance, 231  
**Cybercrime**, **3**, **4**, 91  
    Advantages of, 11  
    Target, 5  
Cybercrime statistics, 90  
Cybercrimes  
    Count, 5  
    Targets, 5

## Index

- Cybercriminals, 117
- Cyberespionage, 4
- Cyberheist, **xvii, 4**
- Cyberscamming, 17
- Cyberterrorism, 4
- Cyberwarefare, 4
- Dark figure of crime, **92**
- Defamation, 4
- Defense in depth, **193**
- Defense in Depth, **224**
- Defense-in-depth, 224
- Denial of service, **7, 13**
- Denial of Service, **13**
- Department Store Fraud, 115
- Digital certificates, **216**
- Discount scams**, 144
- Distributed denial of service, **135**
- Distributed Denial of Service, **13**
- DKIM, 228
- DMARC, 228
- Domain Keys Identified Mail, 228
- Domain-Based Message Authentication, Reporting & Conformance, 228
- Door security**, 206
- Drive by downloads, **10**
  - Browser Extensions, 34
- Drive-by download, 27
- Drive-by downloads, **9, 33**
- Dropper**, 10
- Ecommerce fraud, 111
- Economic scams, 91
- Educational policy**, 201
- Electronic Funds Transfer Act, 14
- Electronic funds transfers, 14
- Elevated privileges**, 212
- Email account renewal scams, 11
- Email scams, 9
- Encrypting**, 160
- Encryption**, **193**
- Endpoints, 224
- Enforcement policy**, 200
- Extortion**, 232
- Facebook, 106, 152
  - Videos, 153
- Fake access points (APs)**, 68
- Fake antivirus software, 91
- Fake blogs, 154
- Fake File Attachment, 53
- Fake receipts, 146
- Fake websites, 21
- Fake Windows product activation screen, 158
- Financial scams, 91
- Firefox, 191
- Firewalls, **193, 225**
- Follower**, **150**
- Foreclosure fraud, 127
- Foreclosure scams**, 11
- Forensics investigation**, 232
- Fraud**, **17, 91**
  - Avoiding, 119
  - Reasons, 24
- Fraud Detection, 135
- Funds transfer fraud, **84**
- Gartner, 89
- Gift card exchange scams, 143
- Gift card fraud, 115
- Gift card scam protection, 147
- Gift card scams, 142
- Gift cards, 155
  - Unused, 143
- Global online population, 3
- Google Chrome, 191
- Harvest, **9**
- Harvesting, 9
- Hate speech, 4
- Health checking, 220
- Health insurance fraud, 21
- Healthcare fraud, 18
- Healthcare scams, 91
- Heuristic detection, **110**
- Hitman scam, 91
- Home advertisements, 152
- Housing and Urban Development, 125
- HTML5, 33
- IC3, 4
- Identity theft, 18
- Information security practices**, 209
- Insecure computer, 215
- Instant messaging, 153
- Insurance scams, 21
- Internet cafes, 194
- Internet of Things, 36
- Internet use statement, 204
- Intrusion detection system**, 217
- IoT, 36
- iTunes, 134
- Java, 34, **47**
- Java applets, 33
- JavaScript, 33
- Kevin Mitnick, 241
- Keylogger, **8, 10**
- KnowBe4 Security Awareness Training, 243
- LastPass, 227
- Lawsuits**, 232
- Least privilege, 212
- Legal
  - Online Crimes, 17
- Legal jurisdiction, 12
- Libel, 4
- LinkedIn, 154
- Locking out, 158
- Logoff, 186

- Loss or Damage to Reputation**, 232
- Losses to the Business**, 232
- Malicious Attachment, 50
- Malicious extensions, **47**
- Malicious hyperlinks, 149
- malvertising**, 159
- Malvertising, **35**
- Malware, 9
- Malware infections, 91
- Man-in-the-middle attack**, **225**
- MFA, 167
- Microsoft Defender, 227
- Microsoft Edge, 191
- Mobile, 99
- Mobile banking fraud**, 68
- Mobile email downloads**, 68
- Mobile threats, 169
  - Data leakage, 172
  - Lost phone, 172
  - Malicious applications, 170
  - Phishing, 171
  - PIN Number, 169
  - Public Hotspots, 170
  - Security vulnerabilities, 171
  - Spyware, 172
  - Stalkerware, 172
- Money mules, **108**, 134
- MoneyGram, 134
- Monitoring plan, 205
- Monitoring policy**, 200
- Mortgage escrow fraud**, 123
- Mortgage rescue scams, 121, 125
- Mortgage scam, 123
- Mozilla Firefox, 191
- Mules, 14
- Multifactor authentication**, 187
- Multi-factor authentication, **86**
- Multi-Factor Authentication, **187**
- Multi-Factor Authentication Security Assessment, **187**
- National Cyber Security Awareness month, 240
- Nigerian scam, **20**, 22, 92
- NTFS**, 210, 215
- NTFS permissions, 211
- Number harvesting**, 65
- NW3C, 4
- Office supply scams**, 144
- Offshore, 14
- One-factor authentication, **187**
- Online Crimes, 17
- Online job scams, 91
- Online merchant fraud, 111
- Online merchants, 117
- Online reputation**, **229**
- Online SAT, 242
- Packet analyzer**, **194**
- Password safety**, 188
- Passwords, 187, 188
  - Weak, 23
- Patch Tuesday, 221
- Patches, 221, 226
- patching, 167
- Payday loans, 11
- Payments fraud**, 130
- PayPal, 116, 118, 119, 134, 146
  - ACH Scams, 131
- PayPal's Buyer Protection policy, 118
- Payroll fraud, 108
- Permissions, 210
- Phantom help scam, 121
- Phishing**, xvii, **7**, **45**
  - Call to act, 77
  - Earliest, **45**
  - Imitation, **46**
  - Luring victims, 58
  - Motivation, **46**
  - Profit, 58
  - Take Action Now, **47**
  - What criminals want, 57
- Phishing attacks, 34
- Phishing messages, 28
- Phishing sites, 33
- Phone number harvesting, **65**
- Phrase techniques, 189
- Phreaking**, **105**
- Physical access policy**, 201
- Physical security, 205
- Physical Security, 186
- Policies, 224
- Ponzi, 22
  - Victims, 24
- Powershell, 160
- Premises monitoring**, 205
- Principle of least privilege, **193**
- Private Label Fraud, 115
- Prizes, 155
- Promotion scams, 144
- Proprietary VoIP, 67
- Protocol analyzer**, **194**
- Proxy server, **115**
- Proxy servers**, 193
- Public PCs**, 194
- Public Shaming**, 166
- Public Wi-Fi network, 194
- Quizzes**, 152
- Ransomware**, **6**, **10**, **157**
  - Bitcoin, 36
  - History, 157
- Ransomware Insurance, 160
- Ransomware-as-a-Service, 160

## Index

- RDP bruteforce password guessing, 157
- Remote access, 218**
- Retail scams, 141
- Reveton, 158
- Rogueware, 9
- Routing number, 129
- Safe computing, **185**
- Safe surfing, 196**
- SAT course, 242
- Scams, 17
- Scareware, 160**
- Schemes**
  - Debt elimination, 10**
- Screen lockers, 160**
- Search engine**
  - optimization (SEO), 144**
- Security auditing, 214**
- Security awareness, 239
- Security awareness training, **98**
- Security Awareness Training, 240
- Security classifications, 213
- Security policies, 215
- Security policy, 199**
- Security tab, 210
- Security updates, 221
- Security vulnerabilities, 226
- Seller protection, 118
- Sender Policy Framework, 228
- Separation of duties, 214**
- Server room, 212
- Service packs, 221
- Session hijacking, 225**
- Share permissions, 210**
- Smart Devices, 36
- SME, **84**, 90, 103, 111, 131
- Smishing, 61
  - Anatomy, 61
- Sniffer, 194**
- Social engineering, **xvii**, 28, 55, 189
  - Red Flags, **55**
- Social Engineering
  - Spear Phishing, 74
  - Whaling, 74
- Social media, 149
- Social networking, **xviii**
- Social Networking Scams, 149
- Spam, 4, **32**
- Spamming over Internet telephony, 65
- Spanish Prisoner, 21
- Spear phishing, 71, **72**, 99
- Spear Phishing
  - Avoidance, 79
- SPF, 228
- Spoofed, 32**
- Spyware, 195
- Stalkerware, 172
- Steal Credentials, 165**
- Steal or Leak Data, 164**
- Steganography, **49**
- Sting and Grab, 15
- Stolen credit cards, 111
- Stressor, 29
- Surveys, 205**
- Tailgating, 206**
- Targeted attack, 71
- Telephone
  - Attacks, 65
- Threaten Everyone, 166**
- Threaten Victim's Customers, 165**
- Threaten Victim's Employees, 165**
- TLS, 191
- Transport Layer Security (TLS), 190**
- Trojan, **8**
- Trojans, 10, 195
- Twitpic, 155
- Twitter, 106
- Twitter phishing scams, 150
- Two-factor authentication, **138**, 187
- Typosquatting, **143**
- Unpatched browsers, 47
- Updates, 221
- URL shortening, **54**
- USB, 220
- Use Stolen Data to Spear Phish Partners and Customers, 165**
- User education, 204
- User Education, 229
- Username, 187
- Video cameras, 206**
- Virtual machines, 160
- Virtual private network, 218
- Viruses, 195
- Virustotals.com, 138
- Vishing, **61**, **65**, 67
- Voicemail overloading, **65**
- VPN, 218
- Wannacry, 157
- WannaCry, 158
- Web based scams, 143
- Web proxy server, 217
- Webcam Hijacking, 35
- Western Union, 134
- Whaling, **71**
  - Anatomy, 75
  - Avoidance, 79
- Whaling Attacks, **73**
- Wi-Fi networks, 194
- Windows 10
  - Patch update intervals, 221
- Windows Active Directory, 215
- Windows Update, 221
- Wire transfer fraud, 18
- Work- at-home opportunities, 155



Worms, 195  
YouTube, 153

Zeus toolkit, 12  
Zombies, **112**