Contents

About the author xii
Preface xiii
Acknowledgements xv

Introduction: the groups behind cyber attacks 1

01 Phishing 5
Email phishing 6
Business email compromise 9
Phishing phone calls 11
Caller ID spoofing 14
Phishing messages 19
QR code phishing 20
Hybrid phishing 21
Protect against phishing 23
Notes 25

02 Account compromise 30
Passwords 32
How passwords are compromised 34
SMS 2FA 38
Stronger 2FA 39
2FA fatigue 41
Password managers 41
Advice for securing your accounts 43
Notes 45

03 Vulnerabilities and exploits 48
Zero-day vulnerabilities 50
N-day vulnerabilities 52
A vacuum of patches 55
The vulnerability ecosystem 57
Vulnerabilities and different devices 60
Managing vulnerabilities and mitigating exploits 62
Notes 63

04 Romance fraud 67
The psychological strategy of romance scammers 69
When you are the catfish 74
Social media and romance scams 75
The psychology of romance fraud 77
The impact of romance fraud on victims 79
Sextortion: image-based sexual abuse 82
Spotting romance fraud red flags and staying safe 84
Notes 86

05 Cyber fraud 88
What makes a fraudster? 89
The strategy and tactics of a fraud 95
Authorized fraud 98
Unauthorized fraud 100
How criminals cash out: money mules 102
The impact of fraud 105
Fighting fraud: how to stay safe 107
Notes 110

06 Identity fraud 115
The impact of identity fraud on victims 116
The scale of identity theft and identity fraud 119
The tactics of identity fraudsters 120
Identity fraud and cyber crime 123
Avoiding identity theft 125
Notes 127

07 Social media scams 130
Fake people 132
Fake goods 136
Fake influencer opportunities 138
Fake jobs 140
Fake news 143
Surging social media scams 144
Stay social media savvy 146
Notes 149

08 Malicious insiders 154
What motivates malicious insiders? 155
Formula 1 spygate 157
A wake-up call 161
The impact of malicious insiders 163
Malicious insiders and the human side of cyber security 166
How businesses can protect against malicious insiders 167
Notes 168

09 Malware 170
Worms 171
Viruses 172
The global reach of malware 175
Trojans 180
Ransomware 183
Malware-as-a-Service 185
Spyware 187
Protecting against malware 189
Notes 190

10 Ransomware 193
Cryptocurrency 194
An evolving ransomware business model 198
Big game hunting in ransomware 199
Escalating extortion 200
Law enforcement whack-a-mole 202
Borders in a borderless crime 203
Insurance, brokers and negotiators 209
To pay or not to pay, is that the question? 210
Ransomware mitigations and managing an incident 212
Notes 214

11 Internet of Things (IoT) 218
Default passwords 220
The Mirai fallout 222
Lessons from Mirai 224
Mirai's legacy 226
Securing the Internet of Things 228

Cyber security in an increasingly connected world 229
Notes 231

12 Cryptocurrency crime 233
Pig-butchering scams 234
Billions of cryptocurrency 237
Cryptocurrency: untraceable money? 239
Cryptocurrency investigations and the return on investment 242
Not all exchanges are equal 244
Staying safe with cryptocurrency 246
Notes 248

13 Artificial intelligence 250
The rise of the machines 253
AI: a force multiplier of fear, uncertainty and doubt 253
Garbage in, garbage out 255
Large language models 257
Deepfakes 261
National and international implications of AI 262
Organizational implications of AI 264
Implications of AI for individuals 265
Plausible deniability 267
Staying cyber safe in an AI age 268
Notes 270

14 Conclusion: staying safe from cyber attacks 273

Index 277