

Index

CAREER

- Crime-as-a-Service (CaaS), 108-109
 - booter sites, 109-110
 - exploit kits, 111-112
- individuals, 98
 - crooks and perps, 100-102
 - money mules, 98, 183-184, *see also* **CLASSIFICATION**
 - rationalizers, 99-100
- organized crime, 102-103
 - criminal and terrorist financing, 102, *see also* **CYBERFRAUD**
 - high-speed cyberfraud, 103-104
 - cyberextortion, 104-106, *see also* **CLASSIFICATION**
 - cyberfraud against banking institutions, 106-107
 - tax fraud, 107-108

COMBATTING CYBERFRAUD

- common tips, 28-29, *see also* **PREVENTING CYBERFRAUD**
- law enforcement surveillance and access to information, 145
 - right to privacy, *see* **CYBERFRAUD**
- opportunities, 146
 - centralized data collection, 153
 - criminal profit centres, disruption of, 153-155
 - environmental factors, 155-156
 - global collaboration, 156
 - data retention laws, 159-160
 - identity fraud, 156-157, *see also* **CLASSIFICATION**
 - illegal online gambling, 157-158
 - law enforcement education and collaboration, 158-159
- increased reporting, 147-149
 - financial institutions, 150-153
 - money mules, 148, *see also* **CLASSIFICATION**
 - organizations and employees, 149
 - scam victims, 147-148

- safeguards and measures, 146
 - compensating procedures, 147
 - corrective measures, 147
 - detective controls, 147
 - preventative safeguards, 147
- successes, 143
 - money laundering, 143-145
 - online pharmacy fraud, 145-146
- technology, 143

CYBERCRIME, *see also* **CYBERFRAUD**

- definition, 8-9
- relationship with cyberfraud, 9-12
- targets, 10

CYBERFRAUD

- definition, 1, 4-5, 8, 28
- different from cybercrime, 7-9, 13-14, 161
 - affiliate programs as a tool for cyberfraudsters, 22-23
 - credit bureaus' use of credit information for marketing, 22
 - currency scams, 18-21
 - cyberheist as a prelude to, 10, 14-15
 - ATM theft, 15-16
 - cyberextortion, 16-17
 - cyberbullying, 17
 - malware, 17
 - ransomware, 16-17
 - enablers as opposed to cyberfraudsters, 8, 21, 39, 161
 - global banks, deceptive activities of, 18
 - government-funded cyberattacks, 24
 - money transfer organizations, 21
- future of, 171
- nature, 60
- personal information, value of, 30
- related problems
 - human rights violations, 125
 - right to privacy, 14, 125, 145, 167
 - violence, 125

- Proceeds of Crime (Money Laundering) and Terrorist Financing Act, see LEGISLATION*
- terror funding, 102, 125-126, 145, 156-157, 214
- roots, 49
- long con, 52-53
 - Spanish prisoner scam and advance fee fraud, 53-56, 94, *see also* **CLASSIFICATION**
 - money laundering, 56-58, *see also* **CLASSIFICATION**
 - Ponzi scheme, 58-60, *see also* **CLASSIFICATION**
 - short con, 49-50
 - chain letter and email and social media fraud, 50-52, *see also* **CLASSIFICATION**
- social network scams, 33
- why it works, 61-62
- anonymity of the Internet, 61
 - human nature, 61-62

CLASSIFICATION

- Cyberfraud Classification Framework, 33-34, 181
- categories, 34-36, 179-180
 - advance fee fraud (**Category H**), 44, 53-56, 67
 - inheritance fraud, 201, 213
 - 419 inheritance fraud, 213-214
 - fraudulent cheque, 201-202
 - mortgage/loan fraud
 - chief scam, the, 222-223
 - fraudulent lender, 198-199
 - Internet real estate scam, 197-198
 - online loan scam, 185
 - Nigerian/419 fraud, 44-45, 91, 94, 118, 122-123, 125, 138, 168, 172, 203
 - Canadian 419 scam, 208-209
 - cheque scam, 226-227
 - legal representation, 203
 - smishing or advance fee fraud through SMS, 240
 - spam marketing and false representation, 263-264
 - stranded traveler scam, 55-56, 64
 - pattern (Tease, Please Seize and Squeeze), 67-68

- phony job offers and business opportunities, 46-47
 - cheque fraud, 256
 - cheque scam, 226-227
 - mystery shopper fraud, 264-265
 - phony criminal record check, 204-205
 - reshipping scams, 266-267
- prize/lottery fraud
 - fake lottery, 190, 223
 - sweepstakes scam, 196
 - telemarketing fraud, 210-211
- ransomware and cyberextortion
 - brand impersonation, 211
 - drive-by extortion malware, 258-259
 - non-crypto-ransomware, 242-243
 - online extortion under threat of embarrassment, 244-245
 - ransomware, 219-220
 - sextortion/webcam blackmail scams, 225-226
- romance swindles, 45, 67, 116-119, 215
 - deceptive online dating practices, 200, 230-231
 - deceptive relationships, 215
 - online dating scams, 243-244
- e-commerce fraud (**Category B**)
 - fraudulent promoters, 38-39
 - mobile phone fraud, 211-212
 - online travel fraud, 196-197
 - seller-side non-shipment, 207-208
 - spam marketing and false representation, 263-264
 - malicious ad networks, 37-38
 - ad fraud, 232-233
 - click fraud, 183
 - online advertising fraud, 246-248
 - online auction fraud, 186-187
 - buyer-side online shopping fraud, 221-222
 - seller-side deceptive advertising, 186-187
 - seller-side non-shipment, 207-208
 - skill bidding, 254-255
 - online marketplace fraud, 193-194
 - buyer-side online shopping fraud, 221-222
 - fake online sales, 251-252
 - fraudulent merchant, 188

- internet software piracy scheme, 193-194
- online travel fraud, 196-197
- seller-side non-shipment, 207-208
- seller-side online shopping fraud, 224-225
- online pharmacy fraud
 - illegal sales of medications, 252-253
 - illegitimate medical vendor, 184-185
 - phony online pharmacies, 145-146
- property-related cyberfraud, 190-191, 197-198
 - chief scam, the, 222-223
 - Internet real estate scam, 197-198
 - rental listing scam, 227-228
 - rental scam by fake landlord, 190-191
 - rental scam with on-site visit by authorized landlord representative, 228-229
 - rental scam without on-site visit, 199
 - seller-side non-shipment, 207-208
- email and social media fraud (**Category C**)
 - business email compromise/CEO fraud, 90-92, 130-133
 - corporate financial details, 250-251
 - email account theft and impersonation, 255-256
 - clickbait and chain letters, 50-52, 72-73, 253
 - samples and subscription traps, 253-254
 - social media hoaxes, 72-73
 - deceptive emails and phishing, 39, 73-76
 - brand impersonation, 202-203
 - spam delivered through SMS, 240-241
 - mass marketing and spam, 195-196
 - hitman text messaging scam, 235-236
 - unsolicited commercial spam, 195-196
- financial system abuse (**Category F**)
 - chargebacks and friendly fraud
 - friendly fraud, 256-258
 - overpayment scam, 259-260
 - charitable donations fraud, 188-189
 - fake charity, 188-189
 - CRA scams and telephone extortion, 42
 - deceptively obtaining goods or services, 209-210
 - immigration-related extortion, 241-242
 - telephone extortion and intimidation, 216-217

- credit card fraud, 215-216
 - credit card clickbait, 215-216
 - new account fraud, 201
 - PIN pad theft, 239-240
 - skimming, 218-219, 237-238
 - subscription traps, 206-207
 - using fake identities, 260-261
 - wireless skimming, 262-263
- debit card fraud, 189-190
 - PIN pad theft, 239-240
 - skimming, 218-219, 187-188, 237-238
 - social engineering and keystroke interception, 229-230
 - wireless skimming, 262-263
- health care fraud (**Category I**)
 - fake treatment, 220-221
 - miracle cure scams, 265-266
 - fake victim
 - faking cancer to solicit donations, 261-262
- identity fraud (**Category D**), 40, 70-73, 213
 - impersonation using stolen identity elements
 - identity fraud, 214
 - identity theft after data breach, 234-235
 - instant messaging scam, 231-232
 - stolen personal details, 221
 - takeover of existing account, 185-186
 - synthetic identity fraud, 40, 76-81
- investment and securities fraud (**Category E**), 201
 - internet stock fraud
 - online securities fraud, 186
 - phony investor alert and recovery services, 41-42
 - Ponzi schemes, 200
 - fictitious lawsuit settlement, 200-201
 - paid autosurf program, 203-204
 - pump and dump, 197
 - email spam, 197
 - establishing a shell company for long-term
 - stock manipulation, 238
 - penny stocks, 205-206
 - pyramid schemes, 40-41
 - online shopping hub, 192-193
- money laundering (**Category G**), 56, 143-145

- individual focus,
 - money mules, 68-70, 98, 148
 - online currency exchange, 42-44
 - organizational focus
 - cyberfraud against banking institutions, 106
 - other deceptive practices (**Category J**), 36
 - unauthorized access (**Category A**), 218-219
 - account compromise
 - account takeover, 248-249
 - using stolen credentials, 182-183
 - Botnets
 - Botnet-facilitated attack, 191-192
 - Botnet-related fraud, 217-218
 - definition, 191, 217
 - online advertising fraud, 246-248
 - online spam - Bredolab botnet, 249-250
 - social media botnet, 245-246
 - general malware, 36-37
 - drive-by extortion malware, 258-259
 - money muling, 183-184
 - pretexting
 - bank fraud using phishing emails, 252
 - combined smishing and vishing in text messaging scam, 236-237
 - phishing, 214
 - social engineering and keystroke interception, 229-230
 - technical support scam, 233-234
 - spyware
 - personal activity monitoring, 194-195
 - selective theft of information, 194-195
 - Cyberfraud Reference Library, 181-182
 - how to use, 181-182
 - importance, 25-26
- DETECTING CYBERFRAUD**
- general, 124
 - hiding in plain sight, 125-127
 - how to spot cyberfraud, 127
 - three conditions of fraud, 127-130
 - opportunity, 128-129

- pressure, 128
- rationalization, 129-130
- technology, 126
 - artificial intelligence, 126-127
- under-reporting and inaction by victims, reasons for, 133-134
 - embarrassment, 134, 138
 - ignorance or disincentive, 138-139
 - confirmation bias, 125, 134, 138
 - negative consequences, 139-141
 - prestige effect, the, 135
 - skepticism, 135-137

GLOBAL TRENDS

- Australia, 162-164
 - computer virus scams, 162-163
 - domain name scams, 164
 - energy billing scams, 162
 - fake franchise scams, 163
 - fake ticket scams, 163
 - fake websites, 163
 - impersonation scams, 163
 - romance swindles, 164
 - scareware, 163
 - tragedy scams, 163
 - travel scams, 162
- Canada, 167-170
 - advance fee fraud, 168
 - affinity fraud, 168
 - astroturfing, 167-168
 - curbers, 168-169
 - pretender scams, 169
 - prize/lottery fraud, 169
 - redirection scams, 169-170
 - romance swindles, 168
 - telemarketing fraud, 169
- United States, 164-167
 - arrest warrant scams, 165

- auction reseller scams, 164-165
- casting call/expert interview scams, 165-166
- fake contact scams, 166-167
- foreign currency scams, 166
- home improvement scams, 165
- medical alert fraud, 164
- scam texts or SMS “smishing”, 166

LEGISLATION

Canada

- Competition Act*, 41, 193
- Personal Information Privacy and Electronic Documents Act*, 78
- Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, 148

United Kingdom

- Proceeds of Crime Act 2002*, 148

PREVENTING CYBERFRAUD

FBI’s “Cyber’s Most Wanted” list, 113-114

public education

- importance, 172
- limits to, 136

simple prevention

- avoiding identity fraud, 115-116
- basic tips, 114-115
- failure, reasons for, 116
 - absence of a common language, 123-124
 - emotional investment, 116-119
 - exploitation of public awareness, 122-123
 - illusion of simplicity, 119-122

VICTIMS

individuals, 63, *see also* **CLASSIFICATION**

- predisposition to being scammed, 63-65
- self-selection, 65-66
- sucker lists, 66-67

nations, 94

- Ghana, 84

- Malaysia, 96
- Nigeria, 94
- Romania, 95
- South Africa, 95
- organizations, 81
 - commercial bank fraud, 82-83, *see also* **CLASSIFICATION**
 - bank fraud losses, 83-84
 - cyber loss insurance coverage, 84-85
 - identity fraud, 85-86, *see also* **CLASSIFICATION**
 - impersonating an entity to commit tax fraud, 92-93
 - phishing and social engineering, 86-87
 - business email compromise/CEO fraud, 90-92, 130-133
 - domain name fraud, 87-90
 - how vulnerable, 81-82
 - small business, 93-94