

A

- account, financial
 - compromised, 248
 - phishing schemes, 21–22
 - unused, 242
- accounting reforms, 188
- AccurInt search website, 22
- ActiveX
 - IE exposure, reducing, 212
 - malicious code, sending, 161, 211
 - right-click, disabling, 77–78
 - scripting, disabling, 39
 - security hole, 28
 - Xupiter toolbar, 128
- address bar
 - covering with fake, 79–82
 - planting wrong information, 91–92
 - popups, 83
- address poisoning
 - DNS, 100–101
 - hosts file, changing, 101–103
 - TCP packet bouncing, 103
- administrator log in, avoiding, 218–219, 225
- admissibility, evidence, 196
- advertising, 79, 107
- adware
 - bogus removers, 130
 - computer resources, draining, 124
 - cookies, 214
 - defined, 105, 263
 - spyware, 109
 - trackers and pop-up distracters, 128–129
- Al-Qaeda, 15
- Amazon, 18
- annoyance, 263
- Anti-Phishing Working Group. *See* APWG
- antivirus program, 121, 222–223
- AOL (America Online)
 - email protocol, 156
 - hours, stealing, 4, 18
 - passwords, cracking, 6
 - stolen addresses, 31
- API (application programming interface), 77–78
- applications, logging used, 110
- APWG (Anti-Phishing Working Group)
 - compromised computers in U.S., 19
 - email scams, reporting to, 257

APWG (*continued*)
 information, sharing, 181
 phishing site, time staying up, 20
 phishing targets, 17
 size and increase in phishing
 profitability, 6
ARPAnet, 139
asymmetric cryptography, 93
asymmetric key encryption, 158,
 263–264
ATM cards, faking, 15
attachments, email, 153, 231
attack
 automated nature, 7
 defined, 264
 prototypical, 10–13
 targeted, 20–21
attack response plan
 Defense-in-Depth strategy, 193
 described, 191
 evidence, 195–197
 incident-handling capability, 194
 investigating, 195
 liability issues, 192
 monitoring and auditing, 193–194
 team, 194
attack vector, 124–127, 264
auctions, 237. *See also* eBay
auditing
 attack response plan, 193–194
 defined, 142, 264
 importance of, 22, 238
authentication
 biometrics, 170
 chip and pin, 167
 confusion, 86–87
 customers, 163–170
 defined, 142, 264
 email, 155–159
 European solutions, 166–170
 fingerprint recognition devices,
 fooling, 170

 FinTS, 168
 HBCI, 168
 i-STIK, 169
 mutual, 142–143, 269
 SecurID, 168–169
 TAN, 167–168
 two-factor authentication, 163–166
authenticity, website, 236
authorization, 142, 264
automated phone script, 2
auto-responder, email, 153

B

back ups, computer, 217–218, 220
backdoor, 118, 264
bandwidth, 62, 179–180
banking systems. *See* financial
 institutions
banner ads, removing, 103
bcc (blind carbon copy), 234, 236
benefits, phishing, 5–7
BHO (Browser Helper Object), 128,
 265
biometrics, 170
bits, 94, 96
blackhole list, 125
blacklist, 125, 264
blind carbon copy (bcc), 234, 236
bogus removal programs,
 119–120, 130
bookmarks, unfamiliar, 124
bot net, 14
brands, 123, 137
Brazil, 16
browser. *See* web browser
Browser Helper Object (BHO), 128,
 265
browser hijacker, 116, 267
Bugzilla bug report, 92
bulk mail, 27–28
business. *See* financial institutions;
 organization

C

- CA (certificate authority), 94–95
- cable connections, 62
- Caller ID for Email, 181
- CAN-SPAM legislation, 28, 31
- carding, 4
- Caribbean phishing sites, 63
- carjacking, 146
- Cascading Style Sheets (CSS), 46
- CCIPS (Computer Crime and Intellectual Property Section), 182–183
- cell phones, 134, 164–165
- CERT (Computer Emergency Response Team)
 - attack response plan, 194
 - flaws, identifying, 7
 - IE warning, 211–212
- certificate authority (CA), 94–95
- certificates
 - described, 94–95
 - fraudulent, 139–140
 - spoofed phishing websites, 94–95, 99–100
- chain, evidence, 195–196
- challenge/response secret questions, 165–166
- chargeback, 265
- chat room security token, 169
- child monitoring spyware, 108
- children, chat room security, 169
- China, 19–20, 63
- chip and pin user authentication, 167
- choosing computers, 62–64
- chrome exploit, 92
- CIRT (Computer Incident Response Team), 194, 195
- Cisco Systems IIM, 155, 159
- Citibank
 - name, use of full, 153–154
 - phishing email with good grammar, 46
 - as phishing target, 18
- client-side solutions
 - authenticating users, 163–170
 - browser toolbars, 170–179
- clipboard activity, monitoring, 111
- coding JavaScript, 161
- college keylogging incidents, 115–116
- colors, hiding spam with, 45
- comments, 42, 132
- competition, monitoring, 108
- compromise, 265
- Computer Crime and Intellectual Property Section (CCIPS), 182–183
- Computer Emergency Response Team.
 - See* CERT
- computer forensics, 265
- computer fraud, 265
- Computer Incident Response Team (CIRT), 194, 195
- consciousness, raising consumer, 207–208
- consumers
 - accounts, closing, 248
 - authenticating, 163–170
 - bankers, reassuring, 137–138
 - browser toolbars, 170–179
 - credit report, obtaining, 248
 - detecting phishers, 186
 - educating, 136, 149–150
 - email policies, 152–159
 - identity theft, 248–256
 - logging activities, 246–247
 - passwords, changing, 247
 - phishing, prevalence of, 245–246
 - reporting scams, 257–259
 - website policies, 159–163
- content-based spam filters, avoiding, 40–46
- context menus, disabling, 78
- convenience checks, 241
- cookies, 161, 214
- CoolWebSearch (CWS) browser hijacker, 128

- corporate monitoring spyware, 107–108
- cost
 - customer self-service transactions, 136
 - takedown services, 202
 - to victims, 17
- counterfeit websites, 127
- cousin domains, 52
- cracker, 8, 14, 265
- credentials, copying web, 67
- credit bureaus, contacting, 250–252
- credit cards
 - chargebacks, 136–137
 - fake, creating, 15
 - keyloggers collecting, 109
 - numbers, pretending to have, 53–54, 75
 - preapproved offers, 146
 - purchases with stolen, 4
 - terrorist use of, 15
- credit report, 240, 248
- credit system
 - marketing, 146
 - minimizing exposure through, 241
 - problem, 1–2
 - security flaws, 145
 - Social Security number, use of, 145–146
- criminal cracking spyware, 108
- criminal syndicates, 8, 14–15
- cross-site scripting (XSS), 161
- cryptography, 93–94
- CSS (Cascading Style Sheets), 46
- customers. *See* consumers
- CWS (CoolWebSearch) browser hijacker, 128
- cybersquatting, 52
- cyberterrorism, 207
- D**
- data, backing up computers, 217–218
- Data Protection Act of 1988 and 95/46/EC, 189
- deception schemes, 126–127
- Defense-in-Depth (DID) strategy, 192, 193
- defenses, testing computer safety, 222
- denial of service/distributed denial of service (DoS/DDoS), 265–266
- Department of Justice (DOJ), 182–183
- Department of Motor Vehicles (DMV), 256
- destructiveness, 266
- detecting phishers
 - customer interactions, 186
 - due diligence, 186–187
 - Fair Isaac fraud management solution, 183–184
 - ID Analytics, 184
 - intrusion detection systems, 185–186
 - privacy and legal issues, 187–189
- DID (Defense-in-Depth) strategy, 192, 193
- Digital PhishNet, 182
- DMV (Department of Motor Vehicles), 256
- DNS (domain name system), 100–101, 143–144
- documenting phishing reports, 197
- DOJ (Department of Justice), 182–183
- domain name
 - acquiring, 101
 - hijacking, 116, 143
 - ownership, 199
 - spoofed senders, 52
 - spoofing, 51
- domain name system (DNS), 100–101, 143–144
- DomainKeys headers, 155, 157–159, 181
- DoS/DDoS (denial of service/distributed denial of service), 265–266
- downloadable software, 216

drive-by download, 108, 123, 266
 DSL connections, 62
 due diligence, 186–187, 192
 dumpster diving, 266

E

EarthLink, 157, 171, 173
 eBay
 benefits of using, 23
 link, 34–35
 My Messages localized email, 154–155
 as phishing target, 18
 sample phishing screen, 48, 73
 toolbar, 174–175, 176
 e-commerce, 23, 136
 educating users, 51, 149–150
 electronic transactions, financial, 239
 email. *See also* spam
 attachments, 231
 authentication systems, 155–159
 contents, 232–233
 customer policies, 152–159
 fake return address, 50–53
 forwarding to reporting agencies, 257
 free accounts, as source of phishing, 20
 headers, 233–236
 language, plausible, 46–47
 legitimate, phishing duplicating, 10
 links, 54–59
 mobile phones, sending virus to, 134
 name and number, pretending to have, 53–54
 phishing, received, 1
 plaintext, using, 211
 returned undeliverable messages, 179
 software, choosing safer, 210–211
 spoofing brands, 47–48
 spyware attacks, 125

standard customer communication policy, 152–155
 throughline, 10
 trusting, 230–231
 urgency, suggesting, 48–50
 worm, 266
 email address
 munging email, 36, 119, 269
 whitelisting, 125–126
 employees, monitoring computer activities, 107–108
 end users, 17
 entrapment, 266
 Equifax, 250, 251
 error messages, 75–76
 escrow services, fraudulent, 18
 Europe
 authentication programs, 166–170
 Data Protection Act and amendment, 189
 privacy issues, 184
 evidence, handling, 195–197
 Experian, 250, 251
 exploit, 266

F

FACT Act (Fair and Accurate Credit Transactions Act), 260
 Fair Credit Reporting Act, 240
 Fair Isaac fraud management solution, 183–184
 Falcon Fraud Manager, 183–184
 FBI
 bank Suspicious Activity Reports, 257
 identity theft and terrorism, 15, 255
 keyloggers, 109–110
 FDIC (Federal Deposit Insurance Corporation), 49–50, 137
 Federal Reserve Board's Regulation E, 239
 Federal Trade Commission. *See* FTC

- File and Printer Sharing, 220, 223
 - file extensions, displaying, 225–226
 - filters, spam
 - blacklists, 125
 - filler text, 43–45
 - message, hiding, 45–46
 - oversensitivity, 27
 - trigger words, breaking up, 40–43
 - whitelists, 125–126
 - financial accounts
 - auditing, importance of, 238
 - check cards and debit cards, 240
 - credit, 255–256
 - credit report, auditing, 240
 - credit system, minimizing exposure through, 241
 - identity theft warning signs, 243
 - mailboxes, securing, 242
 - personal information, safeguarding, 239
 - shredding mail, 242–243
 - statements, reviewing, 239–240
 - unused accounts, closing, 242
 - financial institutions
 - accounting and management reform regulations, 188
 - bulk email phishing, benefits of, 27
 - data, privacy of, 188
 - identity theft response, 255–256
 - online statements, 242
 - passwords, changing, 247
 - problems with, 8
 - responsibility for stopping phishing, 8, 137–138
 - as targets, 17–18
 - Financial Services Modernization Act of 1999, 188
 - Finger daemon (*fingerd*), 267
 - fingerprint recognition devices, fooling, 170
 - FinTS (Financial Transaction Services), 168
 - Firefox browser
 - address bar, planting wrong information, 92
 - finding, 215
 - user-agent strings, 88–89, 162
 - firewall
 - installing, 220–222
 - killer, 267
 - spyware limiting, 121
 - First Response Center (FRC), Internet Crime, 202
 - Flash media, 217
 - Flash player, malicious code via, 161, 211
 - foistware, 267
 - forensic evidence handling and preservation, 196–197
 - form, spoofed institution's, 59
 - forwarding email, 159
 - frames, 91–92
 - fraud
 - banking, 138
 - eBay-based, 18
 - identity-scoring systems, 184
 - legal issues, 28
 - fraudulent sites, taking down, 202–203
 - FRC (First Response Center), Internet Crime, 202
 - free email accounts, 20
 - freeware, 267
 - From: address, faking, 50–53, 156, 179
 - FTC (Federal Trade Commission)
 - complaints, breakdown of, 145
 - Identity Theft Affidavit, 252, 256
 - identity theft response, 255
 - phishing scams, reporting, 257
 - relatives, thefts by, 22
- G**
- GAIN (Gator Advertising Information Network), 129
 - Gartner research group, 1, 5, 150

- Google, 102, 175–177, 214
 - government agencies
 - CAN-SPAM legislation, 28
 - CCIPS, 182–183
 - IC3, 183
 - responsibility for stopping phishing, 138–139
 - governmental monitoring spyware, 107
 - grammar, 46, 165, 232
 - Grams – E-Gold Account Siphoner Trojan horse, 133
- H**
- hacker, 8, 267
 - hardening machines, 229
 - hardware
 - backup, 217
 - firewalls, 221
 - infrastructure change, 144
 - keyloggers, 109, 111–113
 - POS chip and pin security, 167
 - removed hard drive, stealing
 - information from, 126
 - spyware, delivering with, 120–121
 - two-factor authentication, 168–169
 - USB two-factor authentication token, 169
 - HBCI (Home Banking Computer Interface), 168
 - H4CK3R* magazine, 16
 - header, email, 233–236
 - help screen, 74
 - heuristic scanning, 222–223
 - hijacker, 116, 267
 - hijacking, 267
 - HIPAA Act of 1996, 189
 - home pages, hijacking, 116
 - honeypot, 185–186, 267
 - hostile ActiveX, 268
 - hostile script, 268
 - hosts file
 - changing, 101–103
 - defined, 132
 - JS/QHosts21-A Trojan horse, 131–132
 - overwriting, 144
 - viewing, 100–101
 - hosts, shutting down, 63
 - HTML (HyperText Markup Language)
 - bogus text, viewing, 232
 - colors, 44
 - customer email, not requiring, 153
 - defined, 268
 - email, 211, 268
 - fake open/close tags, fooling filters
 - with, 41–42
 - filler text, hiding, 45
 - form, spoofed institution's, 59
 - hypertext, 54–57
 - image maps, 45–46
 - images, 48
 - malware, installing, 125
 - source code, stealing, 67–69
 - spam, 35–38
 - HTTP (HyperText Transfer Protocol), 86–87, 90–92
 - hyperlinks, 2, 154
- I**
- IANA (Internet Assigned Numbers Authority), 221
 - IC3 (Internet Crime Complaint Center), 183
 - ICANN (Internet Corporation for Assigned Names and Numbers), 101
 - ICMP (Internet Control Message Protocol), 198
 - ICPCI (Internet Crime Prevention & Control Institute)
 - attack detection phase, 204
 - defined, 182

- ICPCI (*continued*)
 - post-attack phase, 205
 - preparatory phase, 203–204
 - services, 202
 - takedown phase, 204
- ID Analytics, 138, 184
- ID (intrusion detection) systems, 185–186, 193
- identification, 163, 268
- Identified Internet Mail (IIM), 159
- identity theft
 - described, 1, 22, 268
 - phishing and, 146–150
 - warning signs, 243
- identity theft response
 - affidavit, 252, 285–292
 - American time to resolve, 248
 - credit bureaus, contacting, 250–252
 - creditors, contacting, 255–256
 - government agencies, contacting, 255–256
 - hope, maintaining, 259–261
 - letters, sending, 249–250
 - police report, filing, 252–255
- identity-scoring systems, 183–184
- IE (Internet Explorer)
 - address bar, planting wrong information, 90
 - avoiding, 7, 211–212
 - floating JavaScript address bar, 81
 - identifying, 87
 - scripting, disabling, 39, 211
 - sites dependent upon, 215
 - user-agent strings, 162
 - Xupiter toolbar, 128
- IETF (Internet Engineering Task Force), 144, 180–181
- iFrame, 211, 212
- IIM (Identified Internet Mail), 159
- IM (Instant Messaging), 111, 124, 238
- image maps, 58
- images
 - embedded, security issues involving, 211
 - personalized login, PassMark system, 164
 - server solutions, 179–180
 - website, 237–238
- incident-handling capability, 194
- infection, symptoms of, 123–124
- infinite loop, 160
- information, sharing, 66, 180–183, 230
- insider information theft, 259–260
- installing
 - firewalls, 220–222
 - malware, 125
 - patches, 40, 219–220
- Instant Messaging (IM), 111, 124, 238
- Internet
 - attitude toward, 7
 - change, slowness of, 144
 - DNS, fragility of, 143–144
 - mutual authentication, impossibility of, 142–143
 - security holes, 139
 - size and increase of phishing profitability, 6
 - social networks, mining for phish, 232
 - VeriSign seal, 140–141
- Internet Assigned Numbers Authority (IANA), 221
- Internet Control Message Protocol (ICMP), 198
- Internet Corporation for Assigned Names and Numbers (ICANN), 101
- Internet Crime Complaint Center (IC3), 183
- Internet Crime Prevention & Control Institute. *See* ICPCI
- Internet Engineering Task Force (IETF), 144, 180–181
- Internet Explorer (Microsoft). *See* IE

- Internet relay chat (IRC), 124
- Internet Service Provider. *See* ISP
- intrusion detection (ID) systems, 185–186, 193
- investigating attack response plan, 195
- IP addresses
 - bare, 55, 86
 - converting with NAT, 221
 - hosts file, converting, 132
 - intrusion detection system, 185
 - ownership, finding, 200
 - reusing previously compromised, 65
- IP Inspector E-scam (Digital Envoy), 185
- IRC (Internet relay chat), 124
- ISP (Internet Service Provider)
 - email blockers or filters, 119
 - fraudulent sites, taking down, 202–203
 - free email accounts hosting phished data, 20
 - hijacked, 143–144
 - offshore, 203
 - spam, problem for, 27
 - spambot, 119
 - spamming account, shutting down, 28
 - as targets, 18
- i-STIK, 169
- J**
- JavaScript
 - browser behavior, differing, 161
 - coding, 161
 - cookies, 161
 - Firefox dialog box, obscuring, 92
 - floating address bar, 80–81
 - information, verifying, 76
 - right-click, disabling, 77–78
 - rollovers, 57–58
 - security holes, 38, 160, 211
 - websites requiring, 39
- job opportunities, 4
- JPEG (Joint Photographic Experts Group) files, 211
- JS/QHosts21-A blended threat, 131–132
- K**
- keyboards, logging, 113
- keylogger
 - defined, 268
 - family uses, 108
 - hardware, 111–113
 - implanting, 109
 - legality, 109–110
 - process, 110–111
 - rootkit, 114
 - Scob blended attack, 132
 - software, 114
 - U.S. Secret Service alert, 115–116
 - uses, 3–4, 110
- Konqueror browser, 162
- Korgo worm, 12, 131
- L**
- language, plausible in email, 46–47
- law enforcement, 182–183
- legal issues
 - honeypot intrusion detection systems, 186
 - keyloggers, 109–110
 - spam, 28
- letters, sending, 249–250
- liability issues, 192
- license agreement, reading, 216
- life cycle, evidence, 196
- links
 - affiliate, hijacking, 109
 - hiding with JavaScript rollovers, 57–58
 - HTML hypertext, 54–57
 - image maps, 58
 - to original site, spoofed phishing websites, 76–77
 - overuse of, 7

- links (*continued*)
 - relative, 68
 - remove from list, 31
- Linux virus protection, 223
- LMAP (Lightweight MTA Authentication Protocol), 181
- localized messages, 154–155
- logging activities, 194, 246–247
- login pages
 - faking, 70–72
 - linking, 56–57
 - popups, 82–84
 - sources, viewing, 66
- L33t speak, 269
- luring intruders, 185–186, 267
- Lynx browser, 161

- M**
- Mac OS X, 219, 223
- Mail Abuse Prevention System (MAPS), 125
- mail server, 28–30, 234–235
- mailbombing, 51
- mailboxes, securing, 242
- mailing lists, spam, 30–35
- malicious logic, 269
- malware, 91, 269
- man in the middle attack, 148–149, 269
- MAPS (Mail Abuse Prevention System), 125
- MARID (MTA Authentication for DNS), 156–157, 180
- marketing
 - adware, 109
 - brands, spoofing, 47–48
 - credit system, 146
 - Internet, 7
 - scripting email, 387
 - spyware, 107
 - web bug, 31
- mathematics, cryptography and, 93–94, 167
- MD5 security algorithm, 167
- medical information, 126
- merchant chargebacks, 136–137
- message digest, 167
- message, hiding from spam filters, 45–46
- m2g security company, 16
- Microsoft. *See also specific products listed by name*
 - email authentication method, 156–157
 - exploited security flaws, 7
 - patching, 210
- MIME email, 45, 211, 236
- mimicking, 271
- mobile phones, 134, 164–165
- modem phone dialers, 118, 124
- money laundering, 4, 8, 269
- mother's maiden name, faking, 165–166, 247
- Mozilla Web browser, 92, 162
- MTA Authentication for DNS (MARID), 156–157, 180
- mule, 4, 8, 13, 269
- multistage and blended threats, 131–133
- munging, 36, 119, 269
- mutual authentication, 142–143, 269
- My Messages localized email, 154–155

- N**
- naked IP addresses, 86
- name
 - accounts, changing, 218
 - customers, using full, 153–154
 - mother's maiden, faking, 165–166, 247
 - phisher pretending to have, 53–54
- NAT (Network Address Translation), 221
- National Cyber Security Alliance (NCSA), 64, 207–208

- near-miss domain names, 52, 85–86
 - Netcraft toolbar, 177–178
 - Netscape browser, 162, 215
 - Network Address Translation (NAT), 221
 - Nigerian 419 scams, 26
 - *NIX
 - defined, 263
 - malware, 91
 - root account, 219
 - security flaws, 7
 - notary public, 252
 - null character, 90
 - number, pretending to have, 53–54
- O**
- obscuring email address, 36
 - offshore ISP, 203
 - one-way hash function, 167
 - onMouseOver event, 58
 - open relays, 28–30
 - Opera browser, 162, 215
 - operating system, 209–210
 - organizations. *See also* attack response
 - plan; customer
 - information, sharing, 180–183
 - protection focus, 151
 - server solutions, 179–180
 - organized crime, 8, 14–15
 - Outlook (Microsoft), 39, 210–211
- P**
- padlock icon, 79, 100, 140
 - Panix domain hijacking, 143–144
 - paraphernalia, phishing, 14, 18–20
 - PassMark two-factor authentication
 - system, 164
 - passport office, 256
 - passwords
 - AOL, cracking, 6
 - best practices, 226–227
 - changing, 247
 - computer safety, 218
 - remembering, 227–228
 - reset links, 72
 - social engineering to get, 126
 - patches, installing, 40, 219–220
 - Patriot Act scam, 49–50
 - payload, 122, 269
 - PayPal, 17, 88, 153–154
 - peer-to-peer file sharing. *See* P2P file sharing
 - penetration testing, 193
 - personal identification number (PIN), 164, 167, 228, 239
 - Personal Identification
 - Number/TransAction Number (PIN/TAN), 168
 - PGP (Pretty Good Privacy), 94
 - phish, 8, 269
 - phisher, 8, 13–16, 269
 - phishing
 - account fraud, 21–22
 - attack, prototypical, 10–13
 - defined, 1, 9, 270
 - email form, 2
 - hiding from Internet, 23
 - identity theft and, 22, 146–150
 - motives, 5–8
 - paraphernalia, 18–20
 - response plan, 191
 - Trojan horses and spyware, 3–4
 - username and passcodes, obtaining, 20–21
 - phishing email, 9, 270
 - phishing response
 - documenting, 197
 - responsible hosting party, finding, 198–201
 - servers, finding bad, 198
 - steps, 197
 - taking down sites, 201–203
 - phone dialers, 118
 - pictures. *See* images

PIN (personal identification number), 164, 167, 228, 239
PIN/TAN (Personal Identification Number/TransAction Number), 168
PKI (public key infrastructure), 94, 95
plaintext email reader, 37, 55, 232, 270
plug-in applications, mimicking, 122–123
point-of-sale (POS) hardware security, 167
police report, filing, 252–255
popup
 download, 122–123, 270
 in front of real site, 82–84
 URL spoofing, 79
 verisimilitude, 84–85
porn sites, advertising, 128
ports, Trojan horse opening, 117
POS (point-of-sale) hardware security, 167
post office, contacting, 256
P2P (peer-to-peer) file sharing
 attack vector, 124
 disabling, 215
 spyware, installing, 120, 123
preapproved credit offers, 241
predicting numbers, 75
Pretty Good Privacy (PGP), 94
privacy issues
 Data Protection Act of 1988 and 95/46/EC, 189
 GLB Act of 1999, 187–188
 HIPAA Act of 1996, 189
 Sarbanes-Oxley Act of 2002, 188
profile-based anomaly detection, 193
proof of concept, 270
prosecuting identity theft, 5, 150
public key encryption, 158, 263–264
public key infrastructure (PKI), 94, 95
pulling plug, 226

R

RAT (Remote Access Trojan), 118, 270
real domains, spoofed senders using, 51
Real-time Blackhole List (RBL), 125
redirection
 defined, 270
 JS/QHosts21-A blended threat, 131–132
 ports, 117
 servers, 65
 turning off, 84
 unfamiliar site, 124
relatives, thefts by, 22
remembering passwords, 227–228
remote access services, turning off, 220
Remote Access Trojan (RAT), 118, 270
reply addresses, email, 59
reporting scams, 257–259
researching websites, 237
resources, adware using, 124
responsible hosting party, finding, 198–201
retailers as targets, 18
return email address, fake, 50–53, 156, 179
reviews, reading website, 237
right-click, disabling, 77–78
Rivest, Ronald (MD5 algorithm developer), 167
RMX DNS RR and Method for Lightweight SMTP Sender Authorization, 181
Romania, 16
root account, 219
rootkit keyloggers, 114
router, 221

S

Safari browser, 88, 162
Sarbanes-Oxley Act of 2002, 188
Sasser vulnerability, Windows, 12
scambaiting, 26

- scams, common, 9–10
- Scob blended threat, 132–133
- screen. *See also* popup
 - logging, 110
 - website progression, 70–74
- screenshot, 198
- script kiddie, 9, 13–14, 270
- scripting
 - developers, 14
 - disabling browser, 211, 212–213
 - email, 38–40
 - IE address bar, planting wrong information, 90
 - overuse of, 7
 - website, not requiring, 159–160
- seal, images on web pages, 237–238
- search hijacker, 271
- Secure Sockets Layer (SSL), 85–86, 95–99
- Securely Protect Yourself Against Cyber Trespass Act, 108
- SecurID user authentication, 168–169
- security freeze, credit, 241, 248
- security holes
 - credit system, 145
 - Internet, 139
 - JavaScript, 160
- security questions, 72
- security zone system, 39
- SEI (Software Engineering Institute), Carnegie Mellon, 194
- self-service transactions, 136
- Sender ID, 155, 156–157
- Sender Policy Framework. *See* SPF
- sending spam, 28–30
- Sepuc Trojan horse, 125
- server
 - appearance, credibility, 61–62
 - blacklist, 125
 - camping out, 63
 - choosing computers, 62–64
 - compromised, 228–229
 - DNS, 100–101
 - finding bad, 198
 - images, 179–180
 - login links, 56–57
 - mail, 28–30, 234–235
 - multiple sites, 64
 - redirects, 65
 - reusing previously compromised, 65
 - taking over computers, 62
 - URLs, looking for near-misses, 180
 - webjacking, 180
- services, turning off, 202, 220, 223–225
- session key, 96
- short message spam (SMS), 134
- shoulder surfing, 271
- shredding mail, 242–243
- Simple Mail Transfer Protocol. *See* SMTP
- single-factor authentication, 142, 271
- skepticism, 232
- Small HTTP Server, 64
- smart card, 164
- SMS (short message spam), 134
- SMTP (Simple Mail Transfer Protocol)
 - domain keys, 157–159
 - in header, 235
 - IETF proposal, 181
 - SPF, 156
- sniffing, browser, 162–163
- social engineering, 121, 126–127, 271
- Social Security Administration (SSA), 256
- Social Security number
 - credit report blending, 240
 - ease of obtaining, 22
 - fraud, reporting, 256
 - predicting, 54
 - use of, 8, 145–146
- software
 - choosing safer, 208–209
 - downloadable, 216
 - email, 210–211
 - keyloggers, 114
 - license agreement, reading, 216

- software (*continued*)
 - operating system, 209–210
 - P2P file sharing, 215
 - web browsers, 211–215
- Software Engineering Institute (SEI),
 - Carnegie Mellon, 194
- source code, 67–69, 233
- South Korea, 19–20
- spam
 - bulk mail, 27–28
 - content-based filters, avoiding,
 - 40–46
 - defined, 26, 271
 - estimated amount of, 25
 - filter, 271
 - HTML, 35–38, 44
 - legal issues, 28
 - mailing lists, 30–35
 - network bandwidth, overuse of,
 - 26–27
 - Nigerian 419 scams, 26
 - obscuring email address, 36
 - scripting email, 38–40
 - sending, 28–30
 - viruses, 39–40
- spambot, 119, 271
- speed, taking down sites, 201
- SPF (Sender Policy Framework)
 - authentication system, 155, 156
 - header field, 235
 - IETF draft proposal, 180, 181
- SPI (Stateful Packet Inspection), 221
- spoof, 8
- spoofed websites
 - address bar, planting wrong information, 79–82, 90–92, 100–103
 - appearance, importance of good,
 - 66–67
 - browsers, identifying, 87–89
 - certificates, 94–95, 99–100
 - error messages, including, 75–76
 - information, saving, 66
 - links to original site, 76–77
 - near-miss domain names, 85–86
 - popups, 79, 82–85
 - prevalence, 61
 - public and private keys, 93–94
 - right-click, disabling, 77–78
 - screens, progression of, 70–74
 - servers, 61–65
 - source code, stealing, 67–69
 - SSL, 95–99
 - URL spoofing, ease of, 78
 - user authentication confusion, 86–87
- spoofing, 271
- spoofing, email, 155
- SpoofStick browser toolbar, 171, 172
- spyware. *See also* keylogger
 - adware, 109, 128–129
 - attack routes or methods, 124–127
 - bogus removal programs, 119–120,
 - 130
 - browser hijackers and redirectors,
 - 127–128
 - cookies, 214
 - defined, 271
 - described, 105–106
 - drive-by downloads, 108, 123
 - hijackers, 116
 - history, 106
 - increase in use of, 3
 - infection, 2
 - information gathered by, 106–108
 - installing, 120–121
 - Korgo worm, 131
 - multistage and blended threats,
 - 131–133
 - phone dialers, 118
 - pop-up downloads, 122–123
 - prevalence, 106
 - scam throughline, 10–11
 - spambots, 119
 - symptoms of, 123–124
 - Trojan horse, 117–118

viruses versus, 122
 web bugs, 118–119
 SSA (Social Security Administration),
 256
 SSL (Secure Sockets Layer), 85–86,
 95–99
 standard customer communication
 policy, 152–155
 state attorney general offices, 253–254
 Stateful Packet Inspection (SPI), 221
 statements, reviewing, 239–240
 stealware, 109
 switching web browsers, 214–215

T

tables, HTML, 42–43
 taking down sites, 201–205
 taking over computers. *See* zombie
 TAN (transactional access numbers),
 167–168
 targets, 17–18
 TCP packet bouncing, 103
 team, attack response plan, 194
 technical attack, 272
 telephone
 automated phone script, 2
 logging phishing reports, 246–247
 social engineering to get passwords,
 126
 verifying unusual emails, 233
 telephone dialers, 118
 terrorists, 15, 207
 text filler, 43–45
 text, unlocking gobbledygook, 93–94
 throughline, 10
 tokens, 164
 toolbar
 adding, 214
 defined, 272
 EarthLink, 171, 173
 eBay, 174–175, 176
 Google, 175–177

multiple, 178–179
 Netcraft, 177–178
 SpooftStick, 171, 172
 uses, 170–171
 tracking cookie, 272
 trails, audit, 193
 Trans Union, 250, 251
 transactional access numbers (TAN),
 167–168
 trapdoor, 118, 272
 trigger, 272
 trigger words, breaking up, 40–43
 Trojan creation tool, 272
 Trojan horse
 defined, 272
 increase in use of, 3
 JS/QHosts21-A, 131–132
 keylogger, delivering, 109
 prevalence of, 106
 redirecting back to company, 65
 removing, 225
 Sepuc, 125
 spyware, 117–118
 Trojan source, 272
 trusted site, 90
 trusted third party, 94–95
 two-factor authentication
 cell phone SMS messaging, 164–165
 challenge/response secret questions,
 165–166
 defined, 142, 272
 described, 163–164
 PassMark system, 164

U

UK chip and pin security system, 167
 Uniform Resource Locator. *See* URL
 university keylogging incidents,
 115–116
 Unix systems. *See* *NIX
 unused accounts, closing, 242
 urgency, email suggesting, 48–50

URL (Uniform Resource Locator). *See also* redirection
defined, 273
disguising in links, 55–57
near-misses, scanning for, 180
popups, spoofing, 79
spoofing, ease of, 78, 139
U.S. Federal Sentencing Guidelines, 187, 192
U.S. Secret Service keylogger alert, 115–116
USB two-factor authentication token, 169
user accounts, renaming, 218
user-agent strings, 88, 161–163
username and passcodes, obtaining, 20–21
users. *See* consumers

V

VBScript, 161, 211
vector of attack, 124–127, 264
VeriSign seal, 140–141
virus
defined, 273
mobile phones, 134
scripts, spreading through, 39
social engineering, 127
spam, 39–40
spyware versus, 122
unexpected attachments, 231
Visual Basic, 38, 39
vulnerability, 273

W

Wannabrowser tool, 199
warhead, 122, 269
warning signs, identity theft, 243
web browser. *See also* toolbar
address bar, planting wrong information, 91–92
common certificate authorities, 96

context menus, disabling, 78
cookies, disabling, 214
hijacking, 116, 127–128
identifying spoofed phishing websites, 87–89
IE, avoiding, 211–212
JavaScript security issues, 160–161
redirectors, 127–128
scripting, disabling, 212–213
switching, 214–215
toolbars, adding, 214
web bug, 31, 118–119, 273
web mail, 273
web palette, 44
webjacking, 180
webmail addresses, 52–53
WebMoney Trojan horse, 133
websites
authenticity, 236
copying, 48
customers, 159–163
hosts, 19–20
JavaScript, 160–161
logging accessed, 110
phish-in-a-box tools, 14
pictures, 237–238
recommendations, 159–160
researching, 237
reviews, reading, 237
scam throughline, 10
scripting required by, 39
user-agent strings, 161–163
XSS, 161
whitelist, 125–126, 274
Windows Messenger Service (Microsoft), 223–225
Windows (Microsoft)
antivirus program, 222–223
attack vectors, most common, 124
backing up computer, 217
file extensions, displaying, 225–226
problems specific to, 222–226

- right-click, disabling, 77–78
 - Sasser vulnerability, 12
 - security holes, 209
 - services, disabling, 223–225
 - services, turning off, 220
 - spyware and Trojan horses, removing, 225
 - Windows XP (Microsoft), time to infiltrate, 208
 - Windows XP Security Pack 2 (Microsoft)
 - firewall inadequacy, 220
 - installing, 210, 212
 - macro link, 39
 - Witty worm, 209
 - Word (Microsoft) macro link, 39
 - worm
 - developers, 14
 - Korgo spyware, 12, 131
- X**
- XSS (cross-site scripting), 161
- Y**
- Yahoo! DomainKeys headers, 157–159
- Z**
- zombie
 - estimated number, 19–20
 - network, 14
 - servers, 62
 - Zone Alarm Personal Firewall, 106
 - zones, IE security, 39

