

# Index

---

## • A •

- ABC (activity-based costing), 73–75, 78
- active scripting, 341
- ActiveX
  - browser holes, 40, 230, 314
  - defined, 47, 341
  - flagging, 175
  - hard drive, accessing, 44
  - programs, executing, 43
  - scumware, 39
- Ad-Aware Professional SE (Lavasoft), 296–297
- address. *See* e-mail address
- administrative tasks
  - deploying software, 188
  - documentation, 185–186
  - measuring early results, 186–187
  - quarantined mail, 211
  - reporting requirements, 329–330
  - spam filter reporting requirements, 30, 338
  - spyware filter reporting requirements, 340
  - testing, 183
  - time estimates, 183–184
  - trial users, migrating, 183
  - users, notifying, 182
  - validation, 184
  - vendor, involving, 186
- administrators
  - business processes, 104
  - diagnostic skills, honing, 146
  - general interface and functions, requirements for, 329
  - need for training, 144
  - perspective, 145
  - practicing methods, 145–146
  - references, finding, 127
  - skills, evaluating, 26
  - spam filter interface and functions, requirements for, 337–338
  - spam filter training, 282
  - spyware filter interface and functions, requirements for, 340
- adware, 38
- age, trimming quarantine based on, 213
- alarms, managing, 331–332
- algorithm upgrades, 30
- Allman, Eric (writer of sendmail), 244
- allowing mail from certain addresses.  
*See* whitelist
- Altiris patch toolset, 255
- Anti-Phishing Working Group, 312
- anti-popup software, 258
- anti-spam solution. *See* spam filter
- anti-spyware solution. *See* spyware blocker
- antivirus software
  - described, 341
  - as part of defense in depth, 256–258, 341
  - scanner, 180
  - security patches, 253
  - servers, where to place, 21
  - spyware, 14
- appliance
  - CipherTrust IronMail, 272
  - compared to other anti-spam solutions, 31, 117–119
  - described, 167, 341
  - rounding up, 160
  - spam-filtering program, 29, 109–110, 112–113
- application. *See* software
- architecture, 89, 90–92, 156, 341
- ASP (Application Service Provider)
  - backout plan, 283
  - compared to other anti-spam solutions, 31, 117–119
  - described, 341
  - disaster, planning for, 151–152

ASP (Application Service Provider)

*(continued)*

FrontBridge TrueProtect Message Management Suite, 273

implementation, 181

installation staff, 161

left market, 290

legal issues, 231–232

load testing, 165

outages, 234

Postini Perimeter Manager, 271–272

scheduling, 154

spam-filtering program, 29, 109–110, 113–116

trial, 164

user ID and password, theft of, 87

visiting, 128

assessing situation, 89–94

attachments

e-mail, filtering, 21, 258–259

executable, 67

network and Internet usage policy, 50

attacks. *See* deliberate attacks

author, writing to, 8

## • B •

backdoor program, 65

backout planning, 283

backup, 341

backup plans, spyware blocker, 189

bandwidth, 92–93

Bayes, Thomas (probability inference theorist), 60

Bayesian filtering, 59–60, 209, 341–342

Bayesian poisoning, 342

BHOs (Browser Helper Objects),

47, 314, 342

biff, 13

blackholing. *See* RBL

blacklist

described, 226–227, 342

ineffectiveness of using, 17, 214

blocking mail from certain addresses.

*See* blacklist

blogs, harvesting e-mail addresses from, 54

bot, 65–66, 245–247, 342

Brightmail AntiSpam (Symantec), 270–271

browser. *See* Web browser

Browser Helper Objects (BHOs),

47, 314, 342

browser hijacking, 342

budget, 26–27

business

area of, 225, 261, 294

ASP outages, 234

budget, working within, 26–27

contacts, 214, 284–285

data center management, 104–105

e-mail administration, 104

employees, discussing with, 22–23

helpdesk, 103

hidden costs, 233

information, leaking, 15, 86–87

IT skills, evaluating available, 26

legal, 231–232

network management, 104

objectives, 90, 93–94, 153, 286

requirements, 98–101

security project costs, justifying, 27–28

spam filter, supporting, 235–237

spammers, users patronizing, 238–239

spyware filters and scanning, 239

survey, conducting, 23–24

technical infrastructure, 24–25

user accounts, managing, 102

user training and orientation, 35, 50–51, 103–104

user workstations, managing, 102–103

users' skills and attitudes, 25–26

buying e-mail addresses, 55–56

## • C •

calendar time, tracking, 162

calls, user support. *See* helpdesk

CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing

Act of 2003), 21–22

capacity, 90, 92–93, 169

- CAUCE (Coalition Against Unsolicited Commercial Email), 308–309
- cell phones, 67–68, 257
- centralized spyware blocking, 119, 120–122
- chainsaw math, 79–80, 342
- change control group, 156
- chat rooms, 260
- choke point, 221
- CipherTrust IronMail appliance, 272
- client-based solutions
  - compared to other anti-spam solutions, 31, 117–119
  - described, 29, 270
  - spam-filtering program, 116–117
- Clipboard, reading, 44
- Coalition Against Unsolicited Commercial Email (CAUCE), 308–309
- code, executable, 230
- colo (Collocation Facility), 342
- communication, 193
- complaints, specific rules to solve, 216–217
- Computer Viruses For Dummies* (Gregory), 48, 292
- computers
  - firewalls, 21
  - non-company, connecting to network, 50
  - taking over other, 65–66, 245–247, 342
- consolidation, spam-filtering market, 263
- consultants rollout plan, 161
- content efficacy testing, 166, 167
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 21–22
- cookies, 43, 47, 314, 342
- cost
  - business requirements, 98
  - e-mail, analyzing, 74–75, 77–78
  - fully loaded, 80
  - security project, justifying, 27–28
  - success criteria, setting, 108
  - value versus, 81
- counter attack, 19, 243
- coworkers
  - grumbling, 191
  - point of view, considering, 142
  - support for spam blocking, 85
  - surveying, 23
- credit card scams, 84
- custodial data theft, 87
- D •
- DARPA (Defense Advanced Research Projects Agency), 64
- data center, 104–105, 260
- data circuit, 75, 342
- deals, negotiating with vendors, 131–132
- Defense Advanced Research Projects Agency (DARPA), 64
- defense-in-depth strategy
  - anti-popup software, 258
  - anti-spyware market, 266
  - antivirus software, 256–258
  - as best option, 16
  - e-mail attachments, filtering, 21, 258–259
  - inbound and outbound filters, 260–261
  - Intranet firewalls, 259–260
  - layers, listed, 251–252
  - security patches, 252–255
  - spam-filtering market, future of, 262–264
  - standards, emerging, 264–266
  - VERFY command, turning off, 259
- deleting
  - bad information from knowledge base, 202
  - non-quarantined mail, 143
  - quarantined mail, 144, 212–213
  - spam, 79
  - spyware files, 299
- deliberate attacks
  - described, 239–240
  - e-mail address verification or listing, 243–244
  - Joe Jobs spamming, 243
  - NDRs, 247–248
  - phishing scams, 248–249
  - spyware, single-target, 249
  - taking over other computers, 245–247
  - viruses, getting blamed for sending, 245
  - viruses in spam, 14
  - Web bugs and other malicious content, 240–242
  - Web spiders, 244–245
- demilitarized zone (DMZ), 260
- denial-of-service attacks. *See* DoS attacks
- depreciation, 75
- detail level, requirements, 97
- directory service attack (DSA), 56–58, 343
- discussion boards, 54

DLLs (dynamic link libraries), 41, 102–103  
 DMZ (demilitarized zone), 260  
 DNS (Domain Name Service)  
   defined, 343  
   ISP and, 161–162  
   MX records, changing, 180  
   TTL, setting, 181  
 Do Not Spam list, 21  
 documentation  
   spam filter, 185–186, 327–328  
   spyware filter, 327–335, 338–340  
 dollars, converting employee hours to,  
   80–81  
 domain, 229, 343  
 Domain Name Service. *See* DNS  
 DoS (denial-of-service) attacks  
   bots recruiting users' computers, 246  
   defined, 343  
   described, 66  
   outages masquerading as, 220–221  
   TCP, 66  
 downloadable ring tones, 75  
 downloads  
   e-mail addresses, buying and selling, 55  
   network and Internet usage policy, 50  
   software, 41, 315  
 DSA (directory service attack), 56–58, 343  
 dynamic link libraries (DLLs), 41, 102–103

## ● E ●

early warning signs, spam filter problem,  
 190–191  
 economics, 64–66  
 electricity, 75  
 e-mail. *See also* headers, e-mail  
   administration, 26, 104  
   architecture, 24–25  
   attachments, filtering, 21, 258–259  
   centralizing filter for spyware, 121–122  
   client as Web browser, 241–242  
   complex delivery problems, 292–293  
   cost, analyzing, 74–75  
   key logger capturing, 87  
   lost, dealing with, 205–206  
   message origins, hiding by relaying, 62–64  
   message preview, evils of, 240–241  
   personal, 94  
   RBL, 227

  service interruptions, 220–221  
   tagalongs, 41  
   tracking on your own, 235–236  
   volume, ROI model, 76–78  
 e-mail address. *See also* blacklist; whitelist  
   bots, 246  
   buying and stealing, 55–56  
   directory service attacks, 56–58  
   Internet harvests, 54–55, 244–245  
   retaliating for spam, 243  
   verification or listing, blocking, 243–244  
   whois network protocol, 55  
   wrong, 237  
 e-mail volume  
   masking, 293–294  
   ROI calculation, 76–78  
   sizing filter, 32  
   spam and, 12  
   system architecture, 24  
   workload, assessing, 92–93  
 employee-productivity model, 79–81  
 employees  
   business needs, discussing with, 22–23  
   grumblings, reducing, 85  
   offensive language and images, subjecting  
     to, 14–15  
   private information, protecting, 87–88  
 end user. *See* users  
 engine, 218, 343  
 envelope, 229, 343  
 equipment leases, 75  
 escalating problem beyond helpdesk, 148  
 eTrust PestPatrol Anti-Spyware, 299–300  
 EULA (End User License Agreement), 22, 41  
 evaluation, 193, 343  
 Everett-Church, Ray (*Internet Privacy For  
 Dummies*), 309  
 executable programs, 43–44, 314  
 executive frustration, 84–85

## ● F ●

facilities rollout plan, 154  
 false negatives  
   described, 108, 343  
   early results, measuring, 187  
   reporting, 144  
   user expectations, 223–226  
 false positives

abundance, reasons for, 190  
defined, 108, 343  
early results, measuring, 186–187  
low rate and quarantine issues, 287  
spyware filter trial, 174  
user expectations, 226–230  
whitelist, moving to, 17  
Federal Trade Commission (FTC), 21, 310  
file server, 256  
files, removing, 299  
filter. *See* spam filter; spyware blocker  
filter rules  
  described, 343  
  maintaining, 36, 215–217  
  requirements, 330  
  updating, 217–218  
  vendor-supplied, 16  
financial Web sites, 20, 38, 248–249  
fingerprinting e-mail, 273  
fire extinguishers, equating to, 72  
firewall  
  antivirus, 257  
  described, 344  
  inbound and outbound filters, 260–261  
  inbound traffic, blocking, 260  
  Intranet, 259–260  
  protocol holes, 20  
  proxy-based, 180  
  spyware, 14  
  stations, 21  
  TCP connection, configuring, 247  
  worms, 67  
fixed and variable costs, 75–76, 78  
forensic dumping, 242  
forensic study, hard drive, 238  
forgery, 344  
fraud prevention scams, 84  
From: address. *See* headers, e-mail  
FrontBridge TrueProtect Message  
  Management suite, 273  
FTC (Federal Trade Commission), 21, 310  
full installation, spyware blocker, 188  
fully loaded, 80, 344  
functional requirements  
  general, 96–97, 329–332  
  spam filter, 336–338  
  spyware filter, 338–340

## • G •

Gantt charts, 162–163  
gateway filter, 164, 296, 344  
GDI, 242  
geography, computer systems, 24, 260  
GetNetWise, 311  
GFI LANguard, 46  
glossary, user guide, 138  
Google, 43, 258  
grammar, user guide, 139  
graphics  
  illegal, planting onto computers, 242  
  pornographic, 15  
  user guide, 138  
*Gray Matters: The Workplace Survival Guide*  
  (Rosner, Halcrow, and Lavin), 85  
Gregory, Peter (*Computer Viruses For Dummies*), 48, 292  
groups  
  e-mail, turning off, 57  
  harvesting e-mail addresses from, 54  
  IT, 85  
growth needs, 29, 93, 190  
GTUBE (Generic Test for Unsolicited Bulk Email), 167

## • H •

Halcrow, Allan (*Gray Matters: The Workplace Survival Guide*), 85  
hallway grumbling, 191  
hard costs, 233  
hard drive  
  accessing, 44  
  forensic study, 238  
  quarantines filling, 210, 213  
  scanning for spyware, 296, 298–299  
hardware, 160, 180–181. *See also* appliance  
hash, 344  
hash busting, 60–61, 344  
hateful material, 82  
headers, e-mail  
  forging, 61, 344  
  IT, teaching about, 228–229  
  NDR, spammy, 247–248

- headers, e-mail (*continued*)
  - Outlook, retrieving, 199–201
  - SMTP response codes, 236–237
  - tracking, 235–236
  - users, teaching about, 229–230
- headings, user guide, 138
- helpdesk
  - business processes, 103
  - costs of spam and spyware-induced problems, 81
  - described, 344
  - equipping for rollout, 318–319
  - issues, gleaned from users, 196
  - monitoring after implementation, 319
  - productivity, spam draining, 13
  - quarantined mail, 147
  - references, finding, 126
  - repeat calls, reducing, 205
  - screens, viewing users', 198–201
  - staff, evaluating skills, 26
  - support calls, reducing through spyware filters, 86
  - surveying, 23
  - time, allocating during rollout, 155–156
  - too many calls, 288–289
  - training, 146–148
  - updates, looking for, 175
- helper object, 344
- HFNetChkPro, 46
- hidden costs, 233
- home page settings, checking, 314
- HOSTS file, 38, 51, 314
- hours, employee, 80–81
- HTML (HyperText Markup Language), 41, 175, 345
- HTTP (HyperText Transfer Protocol), 121, 175
- human resources department, 105, 151, 157–159
- hybrid solutions, 122–123
- 1 •
- identity theft, 238, 248–249
- IETF (Internet Engineering Task Force), 265
- illustrations, user guide, 138
- IM (instant messages), 67–68, 260–261
- images. *See* graphics
- imaging mail server, 178
- inbound and outbound filters, 260–261
- inbox, 17, 210, 223–226
- incriminating evidence, planting onto computers, 242
- index, user guide, 138
- inertia, user, 141
- information
  - bandwidth, 92
  - knowledge bases, 201–202
  - spam filter implementation, providing, 183
  - too much, handling, 195
  - user support, gaining, 194–197
  - vendors, evaluating, 123–124
- Information Technology. *See* IT
- innovation, spam-filtering market, 264
- inside mail host, 164
- instant messages (IM), 67–68, 260–261
- Internet
  - computers, isolating, 260
  - connection slowness, 293–294
  - e-mail address harvests, 54–55
  - funding, 64
  - spyware infection amnesty, 51
  - usage policy, 50, 315
- Internet Engineering Task Force (IETF), 265
- Internet Explorer (Microsoft)
  - ActiveX controls, problem with, 43
  - Clipboard reading problem, 44
  - configuration, restricting, 230–231
  - graphics library vulnerability, 242
- Internet Privacy For Dummies* (Levine, Everett-Church, and Stebben), 309
- interviewing trial users, 172
- intranet, 140, 259–260
- invisible GIFs, 240
- IP (Internet Protocol), 162, 227, 345
- IRC (chat rooms), 260
- ISP (Internet service provider), 161, 227, 243
- IT helpdesk. *See* helpdesk

IT (Information Technology)  
 business, supporting, 109  
 headers, teaching about, 228–229  
 productivity, spam draining, 13  
 project planning, 33  
 skills, evaluating available, 26  
 trial, setting up, 33–35  
 iterative approach to planning, 150

## • J •

jargon, 139  
 Java, 47, 230  
 JavaScript, 47, 230, 314  
 Joe Jobs spamming, 243, 345

## • K •

Kennedy, Marilyn Moats (*Office Politics For Dummies*), 85  
 key logger  
   corporate information, loss of, 86–87  
   described, 20, 38, 345  
   mechanics, 45  
 knowledge base, 148, 201–202, 345

## • L •

labor costs, 73, 80–81  
 language, approachability in user  
   guides, 139  
 laptops, 21  
 Lavin, John (*Gray Matters: The Workplace Survival Guide*), 85  
 Law of Big Numbers, 221  
 layers, defense-in-depth strategy, 251–252  
 learning style, effective seminars and, 136  
 legal issues  
   ASP use and, 115–116  
   blocked items and, 159  
   business issues, 151, 231–232  
   buying from spammers, 238  
   grievances over offensive material, 14–15  
   ownership of material on company  
     workstations, 316  
   relaying spam, 15  
   rollout, involving personnel, 157  
   spam protection, 292

legislation, 21–22  
 Levine, John R. (*Internet Privacy For Dummies*), 309  
 licensing agreements, 22, 41  
 linear approach to planning, 150  
 load testing, 165, 166, 168  
 log file management, 292  
 logical architecture, 90–91  
 login script, 188  
 long-term vendor product strategies,  
   129–131  
 lost or delayed messages, 289–290  
 low-rate credit card scams, 84

## • M •

mail. *See* e-mail  
 Mail Exchange record (MX record),  
   180, 345  
 Mail Transfer Agent (MTA), 236, 345  
 MailFrontier Gateway Server, 278  
 mailto: link, 244–245, 345  
 maintenance  
   filter rules, 215–217  
   malware filters, 36  
   need for, 209  
   quarantines, 210–213  
   scheduling, 153  
   updates, 217–218  
   whitelists, 214–215  
 malware  
   defined, 5, 16, 345  
   e-mail addresses, finding, 55  
   maintaining, 36  
   spyware versus, 48  
   victims, surveying, 23  
 Mandanis, Greg (*Software Project Management Kit For Dummies*), 33  
 manufacturers rollout plan, 160–161  
 Marimba patch-management product, 255  
 market changes  
   anti-spyware, 266  
   ASP abandonment, 290  
   spam-filtering, future of, 262–264  
   spyware blockers, 49  
 marking quarantined mail, 143  
 MBSA (Microsoft Baseline Security Analyzer), 46

McAfee Anti-Spyware Enterprise Edition Module, 301–302  
 McAfee SpamAssassin, 274–275  
 measuring success  
   spam filter implementation, 186–187  
   spam filter trial, 164–165  
   spyware filter trial, 174  
   user support, 203–206  
 message. *See* e-mail  
 Microsoft. *See also* Internet Explorer; Outlook; Windows  
   security patches, availability of, 253  
   spyware holes, 41  
 Microsoft Automatic Update, 46  
 Microsoft Baseline Security Analyzer (MBSA), 46  
 Microsoft GDI library, 242  
 Microsoft Security Policy Editor, 231  
 Microsoft SMS software, 188  
 Microsoft Windows AntiSpyware, 304–306  
 Microsoft’s “caller ID” through DNS, 265  
 missing e-mail, 187  
 Monty Python “Spam” skit, 13  
 mortgage application scams, 84  
 MTA (Mail Transfer Agent), 236, 345  
 MUD (Multi-User Dungeon) community, 13  
 MX record (Mail Exchange record), 180, 345  
 mysteries, 191

## • N •

navigation, online user guide, 140–141  
 NDR (Non-Delivery Receipt), 54, 247–248, 345  
 negatives, false. *See* false negatives  
 networking, person-to-person, 128  
 networks, computer  
   architecture, 24  
   business processes, 104  
   learning through, 85  
   Microsoft open door problem, 41  
   requirements, 331–332  
   staff, evaluating skills, 36  
   usage policy, 50  
   user ID and password, theft of, 86

new spam techniques, 216  
 newsgroup e-mail address harvests, 54  
 next version, 124–125  
 nonbusiness e-mail accounts, 215  
 Non-Delivery Receipt (NDR), 54, 247–248, 345  
 nondisruptive browser use, 175  
 Norton AntiVirus (Symantec), 300–301  
 Novadigm (HP) computer management product, 255

## • O •

objectives, business  
   assessing, 90, 93–94  
   failure to meet, 153  
   spam filter, reviewing, 286  
 obscene material, 82  
 offensive language and images  
   employees, subjecting to, 14–15, 82  
   inside addresses, bootstrapping, 229–230  
*Office Politics For Dummies* (Kennedy), 85  
 online resources  
   Anti-Phishing Working Group, 312  
   author, contacting, 8  
   CAUCE, 308–309  
   FTC, 310  
   GetNetWise, 311  
   *Internet Privacy For Dummies*, 309  
   IT virtual communities, 85  
   patch management tools, 255  
   ScamBusters.org, 312  
   SMTP reply codes, 237  
   The Spamhaus Project, 307–308  
   SPAM-L Tracking Spam FAQ, 309–310  
   Spychecker, 311  
   SpywareInfo, 310–311  
   Web pages spoofing, update blocking, 46  
 online user guides, 140–141  
 OS (operating system) alterations, cost of, 111–112  
 Outlook (Microsoft)  
   as browser, 241  
   executable attachments, blocking, 67, 259  
   graphics library vulnerability, 242  
   keyword-based spam filter, 61

## • P •

Panda Platinum Internet Security 2005, 302–303

password harvesting, 20, 246

PatchLink tool, 46, 255

PC support staff. *See* helpdesk

PDAs (personal digital assistants), 67–68, 257

peer-to-peer file sharing, 42, 260–261

performance issues

- anti-spam solutions, 30
- described, 220
- Law of Big Numbers, 221
- mail service interruptions, 220–221
- spyware infestation, productivity loss from, 221–222

persistent cookie, 346

personal contacts, users', 214

PERT charts, 162

phishing e-mail

- described, 346
- productivity, draining, 13, 346
- responding, 238–239
- risk-avoidance model, 83–84
- thwarting, 248–249
- Web pages, spoofing, 44–45

physical architecture, 91–92

pictures. *See* graphics

pixel tags, 240

policies

- filtering, 16
- minefields, avoiding, 101
- network and Internet usage, 50
- spam filter, 284
- spyware, updating, 315–316

popup, e-mail, 13

Pop-Up Stopper software, 258

pornography, 14–15, 82

port, 65, 247

Portny, Stanley E. (*Project Management For Dummies*), 33

positives, false. *See* false positives

Postini Perimeter Manager, 271–272

power users, 157

preview, e-mail message, 240–241

pricing. *See* cost

printed user guides, 138–139

privacy issues, 20, 56, 115–116

proactive spyware blocking, 122

probability inference, 60

problem

- anticipating, 149, 151–152
- calls, user support, 205–206
- spam filter, 282–283
- spyware, assessing, 313–314
- testers, 192

programs. *See* software

progress tracking, 193

*Project Management For Dummies* (Portny), 33

project time, tracking, 162

Proofpoint Messaging Security Gateway, 277

protocol holes, 20

punctuation, user guide, 139

## • Q •

quarantine

- administrative maintenance, 211
- automating deletions, 212–213
- choosing test users, 19
- deleting, 144
- described, 17, 346
- end-users, 17, 210–211
- handling, 143–144
- helpdesk and, 147
- huge collections, 210
- managing, 36
- notifying staff, 182
- problems, 169
- user maintenance, need for, 105, 108, 287–288

## • R •

RBL (Real-time Blackhole Listing), 227, 307, 308, 346

redundancy

- advantage of using ASP, 114
- described, 346
- testing, 166
- in training seminars, 137

- references, vendor, 99–100, 125–127, 196
  - Register of Known Spam Operations (ROKSO), 307
  - Registry entries, 47, 314
  - regression testing
    - defined, 346
    - in production environment, 192
    - spam filter, 170
  - regulations, segregating computer systems and, 260
  - reimaging mail server, 178
  - rejected mail
    - RBL, explaining to friends and colleagues, 227
    - SMTP response codes, 236–237
  - relationship, vendor, 129
  - relay
    - bots, 65–66
    - defined, 346
    - Do Not Spam list, feasibility of, 21
    - liability issues, 15
    - message origins, hiding by, 62–64
  - remote access/VPN, 86
  - Remote Desktop Connection, 199
  - repeat calls, helpdesk, 205
  - requirements
    - business, 98–101
    - collecting and organizing, 96, 123
    - described, 94–96, 346
    - detail, necessary, 97
    - functional, general, 96–97, 329–332
    - installation, 335
    - spam filtering, 336–338
    - spyware blocker, 338–340
    - support, 334–335
    - technical, 97–98, 333–334
    - vendor business, 332
  - retaliation, 19, 243
  - review time, 137
  - rhyme, learning through, 136
  - risk-avoidance model, 81–84
  - ROI (return on investment)
    - activity-based costing, 73–75
    - difficulty of calculating, 71–72
    - employee-productivity model, 79–81
    - fire extinguishers, equating to, 72
    - fixed and variable costs, 75–76
    - risk-avoidance model, 81–84
    - volume-of-e-mail model, 76–78
  - ROKSO (Register of Known Spam Operations), 307
  - roles and responsibilities, new, 105
  - rollout plan
    - consulting right people, 150–151
    - disruptive nature of filters, 150
    - objectives, 153
    - problems, anticipating, 149, 151–152
    - resources, allocating, 154–162
    - scheduling, 153–154
    - spam filter trial, 163–173
    - tasks, tracking, 162–163
  - Rosner, Bob (*Gray Matters: The Workplace Survival Guide*), 85
  - rules. *See* filter rules
- S ●
- sales cycles, 131–132
  - salespeople, believing, 124–125
  - SBL (Spamhaus Block List), 227, 308
  - scaling, 29, 190
  - ScamBusters.org, 312
  - scanner, virus, 180
  - scanning
    - proactive filtering versus, 122
    - software, 47–48
    - training users, 50
    - for vulnerabilities, 254
    - Web pages, 140
  - scheduling
    - rollout plan, 153–154, 158–159
    - seminars, 137
    - spam filter implementation, 183–184
    - tracking tasks, 162–163
  - schools, 280
  - scripts
    - computer programming, 47, 230, 314
    - login, 188
    - malicious, masquerading as Web page, 40
    - for user support calls, 202–203

- scumware, 38–39, 346
- search pages settings, checking, 314
- security patch
  - defined, 346
  - importance, 252
  - tools, dedicated, 254–255
  - viruses and worms, 253
  - vulnerabilities, eliminating, 253
- security team, 156, 330–331
- seminars, training, 136–137
- Sender Policy Framework (SPF), 265
- senders addresses. *See* blacklist; whitelist
- sendmail, 62, 244
- server, e-mail
  - anti-spam filters, 30
  - antivirus software, 257
  - denial-of-service attacks, 66
  - full image backup, 178
  - hardware solution, plugging in, 180
  - MTA, tracking, 236
  - NDRs, 54
  - port, limiting, 247
  - spyware, 14
  - storage needs, 78
  - used for relay, 15, 62–64
- servers
  - allocating, 16
  - antivirus software, 256, 257
  - isolating, 260
  - service companies, 280
- Service Level Agreements (SLA), 334–335
- service providers, 161–162
- session cookie, 346
- shared directory, 188
- Shavlik HFNetChkPro security patch
  - tool, 255
- Short Message Service (SMS), 68
- sidebars, 5
- signature
  - upgrades, 30, 239
  - users, training, 50
  - vendor-supplied, 16
- Simple Mail Transport Protocol. *See* SMTP
- simulating spam, 167
- single-target spyware, 249
- SLA (Service Level Agreements), 334–335
- slowness
  - e-mail server, 12
  - Internet connection, 293–294
  - quarantines, overfilled, 210
- SMS (Short Message Service), 68
- SMTP (Simple Mail Transport Protocol)
  - defined, 347
  - illegitimate connections, estimated number, 58
  - port, limiting, 247
  - relaying, 63–64
  - spoofing e-mail, 293
  - standard response codes, 236–237
  - transaction costs, 265–266
  - VERFY command, turning off, 259
- sniffer, 347
- snowflaking, 61, 347
- soft costs, 233
- software
  - compared to other anti-spam solutions, 31, 117–119
  - downloads, spyware hidden in, 41
  - key logger using, 87
  - rollout plan, 160
  - scanning and removing, 47–48
  - spam filter, 29, 109–112, 178–180
  - spyware, executing, 43–44
  - updating, 218
- Software Project Management Kit For Dummies* (Mandanis), 33
- software updates. *See* updates
- Sophos PureMessage, 275–276
- spam
  - company products smell like, 294
  - defined, 5
  - e-mail volume, increasing, 12
  - GDI, 242
  - incoming mail, handling, 143–144
  - Instant Messaging, 67
  - originating from company computers, 15
  - simulating, 167
  - whitelists, maintaining, 144
- spam filter. *See also specific products listed by name*
  - adding, 16–19
  - backout planning, 283

- spam filter (*continued*)
  - Bayesian, 59–60
  - business objectives, reviewing, 286
  - content testing, 167
  - described, 343
  - disaster planning, 151–152
  - explaining, 142–144
  - hash busting, 60–61
  - headers, forging, 61
  - ineffective, 291
  - level, setting, 225
  - lost or delayed messages, 289–290
  - message origins, hiding by relaying, 62–64
  - monitoring after deployment, 285–286
  - policies, reviewing, 284
  - problems, 169
  - quarantines, need for checking, 287–288
  - snowflaking, 61
  - subject lines, teaching users to recognize, 225
  - testing, 285
  - text content, 58
  - training users and administrators, 226, 280–282
  - troubleshooting, 282–283
  - users, evaluating, 279–282
  - vendor out of market, 290–291
  - whitelist, creating global, 284–285
- spam filter implementation
  - ASP, 181
  - documentation, 185–186
  - hardware, 180–181
  - information, providing, 183
  - measuring early results, 186–187
  - plan outlined, 321–326
  - problems, 177–178
  - requirements document, creating, 327–338
  - software, 178–180
  - testing, 183
  - time estimates, 183–184
  - trial users, migrating, 183
  - users, notifying, 182
  - validation, 184
  - vendor, involving, 186
  - watching for trouble, 189–191
- spam filter trial
  - difficulty, 163–164
  - lessons from, 172–173
  - measurable success criteria, 164–165
  - performing, 165–170
  - results, evaluating, 171–172
  - users, selecting, 170–171
- spam, origin of name, 13
- spam relay, 347
- Spam Service Providers, 66
- spam-filtering market, future of, 262–264
- spam-filtering program
  - appliance, 112–113
  - ASP, 113–116
  - client-side solutions, 116–117
  - comparing, 107–110, 117–119
  - software, 110–112
- Spamhaus Block List (SBL), 227, 308
- Spamhaus Exploits Block List (XBL), 308
- The Spamhaus Project, 307–308
- SPAM-L Tracking Spam FAQ, 309–310
- spammers
  - company products smell like, 294
  - economics, 64–66
  - e-mail address verification or listing, blocking, 243–244
  - e-mail addresses, obtaining, 53–58
  - filters, slipping past, 58–64
  - NDRs, 247–248
  - offensive messages in subject lines, 15
  - phishing scams, 248–249
  - retaliation, avoiding, 243
  - specific rules, creating, 216–217
  - taking over other computers, 245–247
  - users buying from, 238–239
  - viruses, 245
  - Web spiders, 244–245
- SPF (Sender Policy Framework), 265
- spoofing, 44–45, 292–293, 347
- SpyBot - Search & Destroy (Spybot S&D), 298–299
- Spychecker, 311
- SpyHunter (Enigma Software Group), 303
- spyware
  - characteristics, 37–40
  - Clipboard, reading, 44
  - cookies, 43
  - corporate information, leaking via, 15
  - defined, 5
  - e-mail tagalongs, 41
  - executing programs, 43–44
  - hard drive, accessing, 44

- infestation, productivity loss from, 221–222
  - installation, 48–52
  - keystrokes, logging, 45
  - legal issues, 232
  - legislation, 22
  - malware versus, 48
  - Microsoft holes, 41
  - network and Internet usage policy, 50
  - patching vulnerabilities, 46
  - peer-to-peer file sharing, 42, 261–262
  - performance issues, 220
  - policies, updating, 315–316
  - problem, assessing, 313–314
  - products, choosing, 316
  - scanning and removing software, 47–48
  - single-target, 249
  - in software downloads, 41
  - spoofing well-known Web pages, 44–45
  - testing for vulnerabilities, 45–46
  - user expectations, setting realistic, 222
  - users, educating, 315
  - utilities, 94
  - Web browser holes, 40, 42, 230–231
  - workstations, keeping from, 20
  - spyware blocker. *See also specific products listed by name*
    - business issues, 239
    - centralized, 120–122
    - characteristics of spyware, 37–40
    - choosing, 28
    - described, 48–49
    - disaster planning, 152
    - easy-to-deploy product, 51
    - e-mail tagalongs, 41
    - hardware, 160
    - hybrid solutions, 122–123
    - market changes, 49, 266, 320
    - models justifying, 85–88
    - software downloads, 41
    - users, training and getting help, 50–51
    - using, 52
    - Web browser holes, finding, 40
    - workstation, 119–120
  - spyware blocker implementation
    - backup plans, 189
    - full installation, 188
    - helpdesk, preparing, 318–319
    - plan outlined, 321–326
    - planning, 317
    - requirements document, creating, 327–335, 338–340
    - watching for trouble, 189–191, 319
  - spyware blocker trial
    - described, 173
    - false positives, identifying, 174
    - installation, 187–188
    - measurable tests and results, 174
    - nondisruptive browser use, 175
    - thoroughness, need for, 317–318
    - users' chores, 174–175
  - SpywareBlaster (Javacool Software), 297–298
  - SpywareInfo, 310–311
  - stakeholders, discussions with, 151
  - standard response code, SMTP, 236–237
  - standardizing spam filter trial results, 172
  - standards, emerging, 264–266
  - stealing e-mail addresses, 55–56
  - Stebben, Gregg (*Internet Privacy For Dummies*), 309
  - stigma, spyware, 51
  - storage capacity problems, 169
  - subject lines, 15, 225
  - support
    - business requirements, 99
    - calls, employee productivity and, 81
    - requirements, 334–335
    - vendors, obtaining, 196–197
  - survey, business needs, 23–24
  - system inventory, 254
  - system whitelists, 215
  - systems testing, 166
- T •
- T1, 347
  - table of contents, user guide, 138
  - TCP (Transmission Control Protocol)
    - described, 347
    - DoS attacks, 66
    - port 25, limiting, 247
    - ports, exploiting, 65
    - source address, viewing, 236

- technology
    - business, 261
    - infrastructure, assessing, 24–25
    - requirements, writing, 97–98, 333–334
    - viewing from user’s perspective, 142
  - telco (telephone company), 347
  - telephone, using to foil phishing
    - scams, 248
  - telnet e-mail spoofing, 292–292
  - test messages, 54
  - testers, 192
  - testing
    - backout plan, 283
    - labs, isolating, 260
    - spam blocker, 183, 285
    - for spyware vulnerabilities, 45–46
  - text content
    - Bayesian filters, 59–60
    - filters, 58
    - misspellings, intentional, 60–61
    - user guides, 139–141
  - text messages, 67–68
  - theft
    - corporate information, 86–87
    - custodial data, reducing through spyware filters, 87
    - employees’ private information, reducing through spyware filters, 87–88
  - Time to Live (TTL), 181
  - To: lines. *See* headers, e-mail
  - training
    - administrators, 144–146
    - Bayesian filter, 60
    - filter, explaining, 142–144
    - helpdesk staff, 146–148
    - knowledge base, building, 148
    - methods, prevalence of, 135
    - online user guides, 140–141
    - printed user guides, 138–139
    - seminars, 136–137
    - spam filter, 226, 282
    - technology, viewing from user’s perspective, 142
    - of trainers, 317
    - user inertia, overcoming, 141
    - users, 35, 50–51, 103–104
  - Transmission Control Protocol. *See* TCP
  - Trend Micro Spam Prevention Solution, 274
  - trial implementation
    - revisiting help desk training, 147
    - setting up, 33–35
    - spyware filtering, 187–188
  - Trojan horse, 21, 67, 347
  - trouble
    - early warning signs, 190–191
    - plan, changing, 191–192
    - in scheduling, 184
    - spyware filter implementation, 189–191, 319
    - testers, 192
    - watching, 189
  - trouble customers, references from, 126
  - trouble ticket, 347
  - troubleshooting spam filter, 282–283
  - TTL (Time to Live), 181
  - Tumbleweed MailGate, 276–277
  - types, user support calls, 204–205
- U •
- UDP (User Datagram Protocol), 65, 348
  - Uniform Resource Locator (URL) spoofing, 44–45
  - unit failure, 166
  - unit testing, 166, 192
  - unrealistic expectations, handling, 190–191
  - unsubscribe links/requests, 55
  - untruths, vendor, 124–125
  - updates
    - browser to block Web site spoofing, 46
    - described, 347
    - maintenance, 36, 209, 217–218
    - requirements, 330
    - users, checking, 175
  - upgrades
    - anti-spam filters, 30
    - described, 348
    - installation, 254
  - URL (Uniform Resource Locator) spoofing, 44–45
  - user accounts, 102
  - User Datagram Protocol (UDP), 65, 348

user expectations  
false negatives, 223–226  
false positives, 226–230  
headers, teaching about, 229–230  
setting realistic, need for, 222–223

user IDs, 20, 86

user support  
answering problems, 194  
communication, progress tracking, and escalation, 193  
information, gathering, 194–197  
measuring, 203–206  
staff, equipping, 197–203

users  
client-side solutions, disadvantages of, 116  
complaints, specific rules to solve, 216–217  
educating about spyware, 315  
evaluating spam filter, 279–280  
filter basics, reiterating, 206  
hallway grumbling, 191  
inertia, overcoming, 141  
interface and functions, requirements for, 329  
issues, gleaning, 196  
preferences, ability to set, 16  
quarantined mail, reviewing, 210–211, 287–288  
questions and issues, anticipating, 147–148  
roles and responsibilities, defining, 105  
screens, viewing, 198–201  
skills and attitudes, evaluating, 25–26  
spam filter interface and functions, 336–337  
spammers, patronizing, 238–239  
spyware blocker interface and functions, 174–175, 339–340  
subject lines, recognizing, 225  
telling about spam filter, 182  
training, 50–51, 103–104, 282  
trial, selecting, 34–35, 170–171  
unrealistic expectations, handling, 190–191  
volume-of-e-mail model, surveying, 77  
whitelists, maintaining, 214, 288  
workstations, managing, 102–103

## • U •

validation, spam filter, 184  
value, cost versus, 81  
VBScript, 230  
vendors. *See also* ASP  
business requirements, 100–101, 332  
customer references, 125–127  
deals, negotiating, 131–132  
filtering rules and signatures, 16  
information, evaluating, 123–124  
left market, 290–291  
long-term product strategies, understanding, 129–131  
networking about, 128  
rescued references, 126  
rollout plan, 160–161  
selecting, 95  
sites, visiting, 127–128  
spam battles, handling, 216–217  
spam filter implementation, 186  
support, obtaining, 196–197  
uniqueness, evaluating, 281  
untruths, 124–125

virus  
calls, tracking, 204  
described, 348  
getting blamed for sending, 245  
scanning, 180  
SMTP relay, planting, 64  
in spam, 14, 66–67

volume-of-e-mail model, ROI, 76–78

VERFY command  
described, 348  
mechanics, 56–57, 244  
server still supporting, 58  
turning off, 259

vulnerabilities  
patching, 46  
scanning, 348  
security patches eliminating, 253  
spyware, testing, 45–46

## • W •

wasted time, estimating, 79–80  
water, 75

- Web beacons, 240
  - Web browser
    - holes, finding, 40, 297–298
    - mail client as, 241–242
    - Microsoft holes, 41
    - popup windows, blocking, 258
    - restricting, 230–231
    - spyware solution, choosing, 51
  - Web bugs and other malicious content, 240–242
  - Web page
    - malicious script, masquerading, 40
    - spoofing well-known, 44–45
  - Web proxy servers, 257
  - Web sites
    - banner ads, replacing, 38
    - cookies, hijacking, 43
    - denial-of-service attacks, 66
    - e-mail addresses, selling, 56
    - hyperlinks to other advertisers', 39
    - malicious code, 82–83
    - popup windows, 258
    - problems accessing, 175
    - tracking use of, 38
  - Web spiders, 54, 244–245
  - whitelist
    - described, 17, 93, 348
    - global, creating, 284–285
    - incomplete, 190
    - maintaining, 36, 144, 214–215
    - service companies, 280
    - system, 215
    - teaching staff about, 182
    - user, 214
    - users not managing, 288
  - whois network protocol, 55
  - Windows (Microsoft)
    - complications, unexpected, 111
    - Outlook header information, retrieving, 199–201
    - Registry entries, 47, 314
    - Remote Desktop Connection, 199
    - update, 46
  - wiretapping laws, 232
  - words, misspelled, 60–61
  - workload, 90, 92–93
  - workstations
    - antivirus software, 256
    - managing, 102–103
    - protection status, 14
    - spyware blocking, 20, 119, 120, 160
    - training users, 315
  - worm
    - described, 348
    - Instant Messaging, 67
    - mass-mailing, 55, 67
- X ●
- XBL (Spamhaus Exploits Block List), 308
  - Xupiter spyware, 39
  - X-Windows, 13
- Y ●
- Yahoo!
    - Anti-Spy Toolbar, 303–304
    - “authentication” through DNS, 264–265
    - cookies, hijacked, 43
    - Toolbar popup blocker, 258
- Z ●
- zombie/zombified computers
    - described, 348
    - Do Not Spam list, 21
    - shutting out, 245–247