

# Index

## • Numerics •

- 1900 port, rules blocking, 104
- 2003 Computer Crime and Security Survey, 17
- 2003 Virus Prevalence Survey, 60
- 5000 port, rules blocking, 104

## • A •

- access control. *See also* Norton Parental Control
  - blocking ads for specific accounts, 245
  - blocking spam for specific accounts, 246
  - for Not Logged On account, 240, 248
  - for Restricted User account, 247
  - restricting access to applications for specific accounts, 250, 261–264
  - restricting access to Web sites for specific accounts, 250, 256–260
  - restricting Internet access for specific accounts, 244, 250
  - restricting newsgroup access for specific accounts, 261
  - for Standard User account, 247
  - for Supervisor account, 238
- accounts, NIS
  - ad blocking for, 245
- Adult account, creating, 241, 243
- Adult account, restrictions for, 256–260, 261–264
- assigning Windows accounts to, 240–242, 254
- business accounts, 247–250
- Child account, creating, 241, 243
- Child account, password for, 255
- Child account, restrictions for, 256–260, 261–264
- compared to Windows accounts, 237
- configuring, 244–246
- creating, 56–58, 242–243, 247–249, 254–255
- default accounts, 238–240, 247
- Not Logged On account, 240, 248
- privacy settings for, 244–245
- Restricted User account, 247
- restricting application access for, 250, 261–264
- restricting Internet access for, 244, 250
- restricting newsgroup access for, 261
- restricting Web site access for, 250, 256–260
- separating from Windows accounts, 242
- spam blocking for, 246
- Standard User account, 247
- startup account, choosing, 58, 248
- Supervisor account, creating, 241, 243, 247
- Supervisor account, password for, 238–240
- Teenager account, creating, 241, 243
- Teenager account, restrictions for, 256–260, 261–264
- accounts, Windows, 237, 240–242
- ACK (acknowledgement) flag, 76
- active content, blocking, 140–141
- Activity log, 311–312
- Ad Blocking
  - blocking ads for specific accounts, 245
  - blocking ads from specific Web site, 212–213
  - blocking specific kinds of ads, 213–214
  - enabling and disabling, 212
  - features of, 16, 205
  - identifying ads, criteria used for, 208
  - putting ads in Ad Trashcan, 206–208
  - rules used by, adding, 212–214
  - rules used by, modifying restrictiveness of, 210
  - rules used by, overriding, 210–212
  - rules used by, viewing, 208–210
  - troubleshooting, 283–284
- Ad-Aware (Lavasoft), 329–330
- address book, importing, 54
- ads. *See also* Ad Blocking
  - blocking with Web Assistant, 65
  - security risks of, 204
  - types of ads used online, 204–205
- Adult account
  - application access restrictions for, 261–264
  - creating, 241, 243
  - newsgroup access restrictions for, 261
  - Web site access restrictions for, 256–260
- Ad-ware, 144–145
- Agnitum Outpost Firewall, 226
- Alert Assistant, 81–83
- alert messages. *See also* Norton Personal Firewall; troubleshooting
  - access choices for, 84–85
  - action recommended by, 77
  - action required by, 77–78
  - categories of, 78–80
  - configuring for applications, 88–91
- Cookie Alerts, 80, 216–217

- alert messages (*continued*)
    - disabling for specific events, 83–84
    - displaying details about, 80–83
    - example of, 69–70
    - Internet Access Control Alerts, 78–79
    - intrusion alerts, 94–96
    - IP addresses in, 73–75
    - malicious worm alerts, 131
    - ports and, 22–23
    - Security Alerts, 79–80, 138
    - tracked in log file, 310–311
    - virus alerts, 128–131
  - Alerts log, 310–311
  - Allow Traffic button, 150
  - “always on” connections to Internet, 24
  - America Online, number of e-mail addresses provided by, 192
  - AmiWeb browser, 269
  - analyzer, 28
  - animated images, blocking, 214
  - AnnaKournikova worm, 133
  - Anonymizer program, 191–192, 219, 333
  - anonymously surfing, 191–192, 219, 333
  - AntiSpam. *See* Norton AntiSpam
  - AntiVir Personal Edition, 227
  - anti-virus software. *See also* Norton AntiVirus
    - for laptops, 227
    - Trojan horse posing as, 25
  - AOL Instant Messenger, 123–124
  - AOL@School search engine, 270
  - APIPA (Automatic Private IP Addressing), 74
  - Application activities log, 312
  - application gateway, 70
  - applications. *See also* services
    - access choices for, configuring, 88–91
    - guidelines for blocking versus allowing, 84–85
    - list of, with corresponding ports used by, 75, 111
    - program scans for, 85–88
    - in Quarantine area, 166
    - restricting access to, for specific accounts, 250, 261–264
    - unblocking access to, 92
    - uninstalling before installation of Norton Internet Security, 39–41, 42–43
  - Ask Jeeves search engine, 270
  - attack signatures. *See* signatures, attack
  - attacks. *See also* Intrusion Detection; troubleshooting; viruses
    - back doors, 25, 345
    - blended threats, 326
    - browser hijackers, 326–327
    - buffer overflow attack, 23, 345
    - “cancel” attack, 23
    - covert channel, 324, 345
    - Denial of Service attacks, 19, 20, 21, 321–322
    - detecting, 93–101
    - by dialers, 20–21, 118, 146–147
    - from disgruntled employees, 342
    - Distributed Denial of Service attack, 346
    - DNS spoofing, 346
    - expanded threats, 118, 144–147
    - FTP “bounce” attack, 23
    - hack tools, 147
    - invalid packets, 322–323
    - IP address attacks, 23–25
    - IP spoofing, 25, 347
    - joke programs, 146
    - keystroke loggers, 145
    - man-in-the-middle attacks, 323–324, 347
    - by password crackers, 19–20
    - ping sweeps, 110–111, 324, 347
    - port scans, 22–23, 110–111, 323, 347
    - reporting, 110, 131, 148
    - by script kiddies, 18–19, 348
    - social engineering, 26, 348
    - spyware, 26–27, 144–145, 327, 329–330
    - surveys regarding, 17, 60
    - SYN floods, 322
    - by thieves, 19
    - tracing, 105–111
    - Trojan horse, 25–26, 116, 170–171, 325
    - types of, 21–28, 321–327
    - worms, 15, 116, 131, 324–325, 348
  - AutoBlock list, 99–101
  - Automatic Private IP Addressing (APIPA), 74
  - Auto-Protect feature, Norton AntiVirus, 119–121, 281
  - Away security level, 61
- B •**
- back doors, 25, 345
  - Backdoor.xxxx Trojan horse, 325
  - banner ads, 245
  - bastion host, 71
  - BAT.Sebak Trojan horse, 117
  - Better Business Bureau (BBB), 341
  - Big Picture Book of Viruses Web site, 14
  - BIOS password protection for laptops, 228
  - “black hat” hackers, 19
  - blended threats, 326
  - Block Traffic button, 100, 149–150
  - Bloodhound technology, 121
  - Bonk attack, 94
  - Bootstrap (Bootp) protocol, rules for, 104
  - “bounce” attack, FTP, 23
  - Briere, Danny (*Wireless Home Networking For Dummies*), 233
  - Brilliant Digital, b3d program, 27
  - browser. *See also* cookies; Microsoft Internet Explorer; Netscape Navigator
    - blocking ads based on, 213
    - blocking content, 140–141, 309–311
    - cache for, 295–297, 345
    - checking security of, 136–138, 140
    - for children, 269
    - communications sent to and from, 12–14
    - encryption level of, 280, 339–340
    - History file for, 220, 265–266, 295–297
    - log file tracking history of, 311
    - preventing information sent to Web sites by, 136–141
    - surfing anonymously with, 191–192, 219, 333
    - updating, 338
  - browser hijackers, 326–327
  - Browser Privacy, 136–141
  - Bruce, Walter (*Wireless Home Networking For Dummies*), 233
  - brute force crack, 20
  - b3d program, 27

Buffalo Spammer, 182  
 buffer overflow attack, 23, 345  
 BumperCar browser, 269  
 business  
   attacks by employees, 342  
   computer crimes on, 17, 342  
   employee e-mail, employer's  
     right to view, 200, 342  
   misuse of company  
     resources, 342  
   user accounts for, 247–250

## • C •

Cabir virus, 231  
 cable locks for laptops, 228  
 cache, 295–297, 345  
 “cancel” attack, 23  
 CAN-SPAM Act, 16, 194  
 CD key (product key), 49,  
   52–53  
 cellphones, security for, 231  
 CERT (Computer Emergency  
   Response Team), 133, 351  
 Child account  
   application access  
     restrictions for, 261–264  
   creating, 241, 243, 254–255  
   newsgroup access  
     restrictions for, 261  
   password for, 255  
   Web site access restrictions  
     for, 256–260  
 children, security for. *See also*  
   Norton Parental Control  
   monitoring online activity,  
     265–267  
   password-protecting  
     computer from, 268–269  
   password-protecting files  
     from, 267–268  
   search engines for children,  
     270  
   signing up for services,  
     335–336  
   spam, children receiving, 336  
   Web browsers for children,  
     269  
 China, spam sent from, 202  
 classes of IP addresses, 74  
 CleanSweep, 39  
 company. *See* business  
 Compelson Laboratories,  
   Password Officer, 34–35,  
   333–334

compressed files, scanning,  
   142  
 Computer Fraud and Abuse  
   Act of 1986, 133  
 computers  
   blocking all connections from  
     specific computers, 99  
   blocking specific connections  
     from specific computers,  
     96–99  
   blocking temporarily after  
     intrusion detected, 99–101  
   communications between  
     computers using Internet,  
     12–14  
   connections to, tracking,  
     305–306  
   determining IP address for,  
     74–75  
   number of computers Norton  
     Internet Security installed  
     on, 52  
   password-protecting, 268–269  
   scanned by Intrusion  
     Detection, 94  
   trusted computers in  
     network, identifying,  
     101–105  
 confidential information alerts,  
   80. *See also* privacy  
 configuration messages, 52  
 Connection Keep Alive,  
   297–299  
 Connections log, 276, 305–306  
 constant IP address, 24  
 content blocking, 140–141,  
   309–311  
 Content Blocking log, 309  
 context-sensitive help, 286  
 Convert Host Name to IP  
   Address Web site, 74  
 Cookie Alerts, 80, 216–217  
 Cookie Crusher program (The  
   Limit Software), 332  
 Cookie Pal program  
   (Kookaburra Software),  
   332  
 cookies  
   blocking, 65, 215–216  
   definition of, 214  
   deleting, 295–297  
   HTTP cookie, 346  
   tracked in log file, 308  
   viewing cookies stored on  
     computer, 215

CoolWebSearch browser  
   hijacker, 326  
 covert channel, 324, 345  
 crackers, 19–20, 345  
 Create Accounts dialog box,  
   57–58  
 CyberSleuth Kids search  
   engine, 270  
 cydoor program, 27

## • D •

data bit, 73  
 data packets. *See* packets  
 data part of packet, 72  
 Davis, Peter (*Wireless Networks  
   For Dummies*), 233  
 The DCOMBulator analysis  
   tool, 227  
 DDoS (Distributed Denial of  
   Service) attack, 346  
 DeepSight, 28  
 deface, 345  
 Default security level, 61  
 defragmenting hard drive,  
   41–42  
 Demilitarized Zone (DMZ), 72  
 demon dialers, 20–21, 118,  
   146–147  
 Denial of Service attacks  
   definition of, 21, 321–322  
   by demon dialers, 20  
   Distributed Denial of Service  
     attack, 346  
   by script kiddies, 19  
   destination port, 345  
   dialers, 20–21, 118, 146–147  
   dictionary crack, 20  
   digital certificate, 338, 345  
   digital signature, 345  
 Direct Marketing Association  
   (DMA), Mail Preference  
   Service, 193–194  
 Distributed Intrusion Detection  
   System, 350  
 Domain Name Service (DNS),  
   23, 104, 346  
 domain part of IP address, 73  
 downloaded software, viruses  
   in, 26–27  
 DShield, 109, 350  
 DSL Reports Web site, 67  
 dynamic IP address, 24

## • E •

EarthLink, spam judgements won by, 182

Electronic Privacy Information Center, 33

e-mail. *See also* spam

- attacks on, 23
- blocking private information sent by, 55–56, 218–219, 244–245, 264–265
- employer's right to view, 200, 342
- encrypting, 200
- filters for filing or blocking, 196–197
- folders, clearing, 198–200
- inability to send or receive, 282–283
- laundering of, 200
- opting out of, with Mail Preference Service, 193–194
- outgoing, scanning for viruses, 52
- scams, recognizing, 26, 29–30, 336
- scanning options for, 123
- security of, 181, 197–202
- tracing source of, 201–202
- tracked in log file, 310
- viruses in, 15, 21, 175

e-mail address

- allowed list for, creating, 54
- for author, 7
- concealing, 200
- for junk e-mail, 192–193
- reducing registrations of, 190–191

E-mail log, 310

emergency disk, creating, 158–160

employees, 200, 342. *See also* business

encryption

- browser level for, 280, 339–340
- of cellphone conversations, 231
- of data on laptops, 230
- definition of, 346
- of digital signature, 345
- of files in Quarantine, 166
- key, 347
- of passwords, 32–35

- for PDAs, 232
- Pretty Good Privacy for, 230, 331
- private key, 347
- public key, 348
- using when browsing, 338–340
- for wireless networks, 232

Encrypt-it! program, 232

errors. *See* alert messages; troubleshooting

Errors log, 312

event logs. *See* log files

Excel files, scanning, 143–144

.exe file extension, 70, 81

expanded threats, 118, 144–147

Explorer (browser). *See* Microsoft Internet Explorer

Explorer, Windows, displaying Norton AntiVirus toolbar in, 66

Express mode, LiveUpdate, 152–153

eXtensible Markup Language (XML), used by ads, 205

## • F •

Federal Trade Commission Web site, 194

file extensions, scanning for viruses based on, 120–121

File Transfer Protocol (FTP), 23, 346

files. *See also* Quarantine area

- from aborted installation, deleting, 50–51
- cache, 295–297, 345
- compressed, scanning, 142
- deleting unneeded files before installation, 38–41
- History file, 220, 265–266, 295–297
- infected, 27–28
- Microsoft Office files, scanning, 143–144
- password-protecting, 267–268
- recovering after deleting, 291–293
- in Recycle Bin, 290–293
- scanning selected files, 126–127
- wiping (permanently deleting), 293–295

- filters for filing or blocking e-mail, 196–197
- FIN (finish) flag, 77
- firewall. *See also* alert messages; Norton Personal Firewall

  - definition of, 1
  - disabling, 47, 340
  - features of, 12–13, 70–71
  - for laptops, 226–227
  - location of, on network, 71–72
  - packet filtering by, 70, 72–73, 75–77
  - reasons for, 14
  - rule base for, 348
  - testing, 227
  - Windows Internet Connection Firewall, 47, 274–275

- firewall appliance, 346
- Firewall log, 306
- Firewall-Wizards mailing list, 352
- FIRST (Forum of Incident Response and Security Teams), 351
- flags, 13, 76–77, 346
- Flash animations, blocking, 214
- forensics, 346
- forms, blocking private information sent by, 55–56, 218–219, 244–245, 264–265
- fragment, 346
- fragmentation, 41, 346
- Froogle Web site, 228
- FTP “bounce” attack, 23
- FTP (File Transfer Protocol), 23, 346

## • G •

gateway, 12, 70

Gibson Research Corporation Web site, 227

Global Teck Web site, 231

G-Mail, free e-mail address provided by, 192

Google Answers service, 288

GriSoft AVG Free Edition, 227

Guest account, 242

## • H •

hack tools, 118, 147  
 hackers. *See also* attacks  
   definition of, 346  
   reporting, 110  
   tracking after an intrusion,  
     105–109  
   types of, 18–21  
 handheld devices, security for,  
   231–232  
 hard drive  
   cleaning up before  
     installation, 38–41  
   defragmenting, 41–42  
   password for, on laptops, 228  
 header of data packet, 72,  
   76–77  
 Help system, 284–286  
 HFNetChk program, 338  
 Hijack This (SpyChecker), 333  
 history of browser activity  
   History file, deleting, 220,  
     295–297  
   History file, viewing, 265–266  
   Web History log, 311  
 Home security level, 61  
 Homework Planet search  
   engine, 270  
 Hotmail, free e-mail address  
   provided by, 192  
 HotSpotVPN service, 233  
 HTML (HyperText Markup  
   Language), used by ads,  
   205  
 HTTP cookie, 346  
 HTTP (HyperText Transfer  
   Protocol), 23, 346  
 Hurley, Pat (*Wireless Home  
   Networking For Dummies*),  
   233  
 Hushmail service, 200  
 hyperlink, 205

## • I •

I Love You virus, 133  
 IamBigBrother software, 267  
 IANA (Internet Assigned  
   Numbers Authority) Web  
   site, 75, 276  
 ICMP (Internet Control  
   Message Protocol), 75–76,  
   103, 347

icons used in this book, 6–7  
 ICQ, virus scanning for, 124  
 ICSA Labs, 2003 Virus  
   Prevalence Survey, 60  
 identity theft, 19–20, 26, 30  
 iJen Software, ScreenLock Pro,  
   334  
 images, animated, blocking,  
   214  
 Import Address Book dialog  
   box, 54  
 inbound communications, 13  
 Incidents Web site, 350  
 Inetinfo.exe application, 84  
 Inoculation feature, Norton  
   AntiVirus, 122  
 Install Over Previous and  
   Current Versions feature,  
   298  
 installing Norton Internet  
   Security  
   initial virus scan for, 46–48  
   post-installation tasks, 53–60  
   preparation for, 37–46  
   reconnecting to Internet  
     after, 60–61  
     setup for, 48–51  
   troubleshooting, 50–51  
   when computer is infected  
     and won't start, 43–44,  
     50–51  
 instant messages, scanning,  
   123–124  
 Interactive mode, LiveUpdate,  
   152–153  
 Internet  
   “always on” connections  
     to, 24  
   blocking connection to  
     immediately, 149–150  
   communications between  
     computers using, 12–14  
   configuring application  
     access to, 88–91  
   connecting in different  
     locations, security  
     settings for, 60–61, 66,  
     222–225, 229–230  
   connecting to Web sites,  
     inability to, 274–280  
   connection to, for  
     LiveUpdate, 153  
   connection to, keeping alive,  
     297–299  
   connection to, tracking,  
     305–306

network activity, tracking,  
   317  
 reconnecting to, after  
   installation, 60–61  
 restricting access to, for  
   specific accounts,  
   244, 250  
 scanning for applications  
   that connect to, 85–88  
 security levels for, 61  
 temporary Internet files,  
   deleting, 219  
 Internet Access Control Alerts,  
   78–79, 84  
 Internet Assigned Numbers  
   Authority (IANA) Web  
   site, 75, 276  
 Internet Connection Firewall,  
   disabling, 47, 274–275  
 Internet Control Message  
   Protocol (ICMP), 75–76,  
   103, 347  
 Internet Explorer (Microsoft).  
   *See* Microsoft Internet  
   Explorer  
 Internet Information Server, 84  
 Internet Protocol. *See* IP; IP  
   addresses  
 Internet Security Systems Web  
   site, 25  
 Internet Storm Center, 350  
 interstitial ads, 204  
 intrusion, 347. *See also* attacks  
 Intrusion Detection  
   AutoBlock list for, 99–101  
   blocking all connections from  
     specific computers, 99  
   blocking connections  
     temporarily after  
     intrusion detected,  
     99–101  
   computers scanned by, 94  
   deactivating, 96  
   definition of, 347  
   excluding signatures from  
     monitoring, 95–96  
   features of, 93–94  
   intrusion alerts sent by,  
     94–96  
   Restricted Zone for, 99  
   signatures detected by  
     Norton Personal  
     Firewall, 94  
   turning off notifications of  
     blocked connections, 96  
 Intrusion Detection log, 307

intrusion signatures. *See* signatures, attack

invalid packet attacks, 322–323

IP addresses

- attacks on, 23–25
- classes of, 74
- determining for your computer, 74–75
- identifying computer to block by, 97
- identifying trusted computers in network by, 102–103
- parts of, 73
- temporary compared to constant, 24

IP (Internet Protocol)

- definition of, 73
- spoofing attacks on, 25, 347
- Version 4 (IPv4), 24, 73–74
- Version 6 (IPv6), 24, 73

ipconfig command, 75

## • J •

JavaScript

- blocking scripts using, 121–122, 140–141, 214
- determining whether browser is running, 136
- used by ads, 204, 205

joke programs, 118, 146

junk e-mail. *See* spam

## • K •

KaZaA, spyware used by, 26–27

Kerio Personal Firewall, 226

key, encryption, 347

keystroke loggers, 145

KidRocket browser, 269

kids. *See* children, security for

KidsBrowser browser, 269

KidsClick! search engine, 270

KidsWeb search engine, 270

Kookaburra Software, Cookie Pal program, 332

## • L •

laptops

- anti-virus software for, 227
- BIOS password protection for, 228
- cable locks for, 228

- creating a new location with associated security settings for, 229–230
- encrypting data on, 230
- hard drive password for, 228
- high-security locations for, creating, 230
- operating system updates, 228–229
- personal firewall software for, 226–227
- protecting from theft, 230
- spam-blocking software for, 228

Lavasoft Ad-Aware, 329–330

Lewis, Barry (*Wireless Networks For Dummies*), 233

license, duration of, 53

license key (product key), 49, 52–53

The Limit Software, Cookie Crusher program, 332

LiveUpdate

- checking for updates after installation, 58–60
- configuring, 67
- enabling or disabling, 124
- Express mode, 152–153
- features of, 28, 151–152
- Interactive mode, 152–153
- Internet connection for, 153
- messages to update software from, 52, 67
- notification of updates by, 154–155
- permitting access by, 85
- privileges required for, 154
- running after malicious worm alert, 131
- running automatically, 154–155
- running manually, 153–154
- Web site restrictions updated by, 265

Local Security Authority Service, 85

localhost connections in log file, 305–306

locations of networks. *See* Network Detector

log files

- attack signatures tracked in, 307
- blocked content tracked in, 309–311

- blocked private information tracked in, 308–309
- blocked traffic tracked in, 306
- blue arrow in, 310
- connections tracked in, 305–307
- cookies tracked in, 308
- definition of, 303, 347
- detecting invalid packet floods with, 322
- disabling logging, 314
- display settings for, changing, 315
- emptying, 162–163
- gold rectangle in, 310
- green circle in, 308
- identifying proxy server ports in, 276
- list of, 304–305
- Norton AntiVirus activity tracked in, 311–312
- Norton Internet Security activity tracked in, 311
- referrer information tracked in, 308
- refreshing, 313
- saving, 313–314
- size of, changing, 314–315
- viewing, 304–311
- Web history tracked in, 311
- “X” in, 308

Log Viewer, Norton AntiVirus, 132

logging on and off, 244

loopback rules, 104

Love Bug virus, 133

lsass.exe application, 85

## • M •

Macintosh, attacks on, 26

macro virus, 27–28

Mail Preference Service, 193–194

mailing lists, 351–352

MailWasher Pro, 228, 332

main window, using, 62–68

malicious worm alerts, 131

malware, 14. *See also* viruses

man-in-the-middle attacks, 323–324, 347

Melissa virus, 133

messages. *See also* alert messages; e-mail for configuration, when opening Internet Explorer, 52

- for LiveUpdate, 52, 67
  - for Norton AntiVirus, when sending e-mail, 52
  - ping messages, 76
  - sent between computers using Internet, 12–14
  - Urgent Attention, in Norton Internet Security, 63
- Messenger
- AOL Instant Messenger, 123–124
  - Microsoft Windows Messenger, 85
  - MSN Messenger, 124
  - Netscape Messenger, 196–197, 198
  - Yahoo!Messenger, 123–124
- Microsoft Excel files, scanning, 143–144
- Microsoft Generic Host Process for Windows 32 Services, 84
- Microsoft Hotmail, free e-mail address provided by, 192
- Microsoft Internet Explorer
- deleting History file, 220
  - deleting temporary Internet files, 219
  - displaying Web Assistant toolbar in, 65
  - enabling ActiveX controls for, 46
  - encryption level problem with, 280
  - putting ads in Ad Trashcan, 208
  - viewing cookies stored by, 215
  - viewing Web history, 265
- Microsoft Office files, 143–144, 268
- Microsoft Outlook Express
- blocking e-mail from single address, 195
  - clearing mail folders, 198–199
  - creating e-mail filters in, 196–197
- Microsoft Printer Spooler Service, 85
- Microsoft TCP/IP Configuration Utility, 85
- Microsoft Windows analysis tools, 227
- Microsoft Windows Messenger, 85
- Microsoft Word files, scanning, 143–144
- More Info link, 286
- Morris Worm, 133
- `msconfig` command, 280
  - MSN Messenger, 124
- N •
- NED.exe program, 159
- ned\_2001.exe program, 159, 160
- NetBIOS service, 23, 104
- Netscape Communicator, viewing cookies stored by, 215
- Netscape Messenger, 196–197, 198
- Netscape Navigator, 220, 266
- Netscape.net, free e-mail address provided by, 192
- Network Detector
- adding networks to an existing location, 223
  - creating a new location with associated security settings, 60–61, 66, 222–224, 229–230
  - features of, 221–223
  - high-security locations, creating, 230
  - modifying security settings, 66
  - viewing and modifying locations, 224–225
- Network Wizard, 101–102
- networks. *See also* access control; accounts, NIS firewall position in, 71–72 identifying trusted computers in, 101–105 reconnecting to, after installation, 60–61 security levels for, 61, 66, 222–223 wireless networks, 232–233
- newsgroups, restricting access to, 250, 261
- newsletters, 352
- Nimda attack, 326
- NIMDA virus, 23
- Nimda\_Propagation attack, 94, 133
- NIS. *See* Norton Internet Security
- Norton AntiSpam. *See also* spam allowed list for, 54, 184, 190 blocked list for, 186–187, 195–196 blocking spam for specific accounts, 246 configuring, 184–190 enabling, 183–184 features of, 16 identification of spam by, 186 level of protection, setting, 185–186 rules for identifying spam, creating, 188–189, 194–195
- Norton AntiVirus. *See also* viruses Auto-Protect feature, 119–121, 281 configuring, 119–124 damaged, 174 disabling, 62 features of, 15–16 Inoculation feature, 122 interfering with installation of Norton Internet Security, 51 log files for, 311–312 Log Viewer, 132 Online Virus Encyclopedia, viewing, 132 scanning, automatic, scheduling, 127 scanning compressed files, 142 scanning, custom, 126–127 scanning e-mail, 123 scanning, full system, 125 scanning instant messages, 123–124 scanning, manual, 122, 124–127, 177 scanning Microsoft Office files, 143–144 Script Blocking feature, 121–122 shortcuts for, removing, 300 timeouts, preventing, 148–149 toolbar for, in Windows Explorer, 66 transferring settings from earlier version of, 298 troubleshooting, 281–282 virus alerts, responding to, 128–131
- Norton CleanSweep, 39
- Norton Internet Security (NIS) activating, 52–53 components of, starting or stopping, 64–66 configuring, 53–60, 66–68

## Norton Internet Security

*(continued)*

configuring to run at startup, 280

configuring to start automatically, 280

context-sensitive help, 286

duration of license for, 53

emergency disk for, creating, 158–160

features of, 1–2, 12–17

Help system for, 284–286

installing, 46–51

installing over previous and current versions, 298

installing, preparation for, 37–46

logging on and off, 244

main window, using, 62–68

number of computers installed on, 52

opening, 51–52, 62

opening, problems with, 280–281

password protection for, 157–158

performance of, improving, 67, 155–156, 192, 204

product key, location of, 49

Professional version compared to home version, 298

RAM requirements for, 40

registration for, 53, 285

shortcuts for, removing, 300

statistics produced by, 316–317

transferring settings from earlier version of, 298

uninstalling and reinstalling, 174, 299–301

uninstalling previous versions of, 42–43

updates for, 58–60, 151–155

Web site for, 11

who should use, 2–3

Norton Internet Security Statistics window, 275–276

Norton Parental Control. *See also* children, security for application access restrictions, setting, 261–264 configuring, 57–58 enabling and disabling, 252–253

features of, 17, 251–252

installation options for, 49

newsgroup access restrictions, setting, 261

requirements for, 253–254

user accounts for, 253–255

Web site access restrictions, setting, 256–260

Norton Password Manager, 32–33, 51

Norton Personal Firewall. *See also* alert messages; firewall access choices for, 84–85 blocking legitimate e-mail, 282–283 blocking specific connections from specific computers, 97–99 checking configuration of, 111 configuring for use with proxy server, 277–278 disabling, 62, 92, 111, 340 features of, 12–13, 70–71, 93–94 identifying trusted computers in network, 101–105 intrusions, detecting, 93–101 intrusions, responding to, 105–111 location of, on network, 71–72 network locations and security levels for, 60–61, 66, 224–225, 229–230 packet filtering by, 70, 72–73, 75–77 program scan, running, 85–91 rules, default, displaying and modifying, 103–105 rules for application access, 88–91 rules for blocking specific connections from specific computers, 97–99 rules for packet filtering, 75–76 rules, priority of, setting, 105, 156 rules, reviewing and modifying, 155–156 rules, tracking rules being used, 317

security levels for, 66

statistics produced by, 106–107, 317

transferring settings from earlier version of, 298

Norton Protection, 290, 291–293

Norton SystemWorks, 39

Not Logged On account, 240, 248

NTBugtraq mailing list, 351



Office (Microsoft) files, 143–144, 268

Office security level, 61

online forms, blocking private information sent by, 55–56, 218–219, 244–245, 264–265

online shopping, security and, 341

Online Virus Encyclopedia, viewing, 116–118, 131

operating system updates, 330, 338

outbound communications, 12–13

Outlook Express. *See* Microsoft Outlook Express

Outlook Express address book, importing, 54



packet analyzer, 347

packet filtering, 70, 72–73, 75–77

packet monkeys (script kiddies), 18–19, 348

packets definition of, 12–13, 23, 347 flags in header of, 76–77 parts of, 72

Parental Control Wizard, 241, 242–243, 254–255

parental controls. *See* Norton Parental Control; Task Lock program

Password Manager, 32–33, 51

Password Officer (Compelson Laboratories), 34–35, 333–334

- passwords  
 as back doors, 25  
 BIOS, for laptops, 228  
 changing, 35  
 for child accounts, 255  
 choosing, 31–32, 337  
 for computer, 268–269  
 crackers obtaining, 19–20  
 encrypting and storing, 32–35  
 for files and folders, 267–268  
 hard drive, for laptops, 228  
 importance of using, 337  
 management programs for, 32–35  
 for Norton Internet Security options, 157–158  
 for PDAs, 232  
 for screen saver, 334  
 for Supervisor account, 238–240  
 for user accounts, 58  
 for wireless routers, 232  
 PasswordSafe service, 33  
 patches, 338  
 PC Magazine, review of  
 password managers, 35  
 PCWorld article about spam, 202  
 PDA Defense, 232  
 PDAs, security for, 232  
 performance  
 ads affecting, 204  
 improving, guidelines for, 67  
 rules affecting, 155–156  
 surfing anonymously, effect on, 192  
 perimeter security, 71  
 Personal Firewall. *See* Norton Personal Firewall  
 PGP (Pretty Good Privacy)  
 encryption, 230, 331  
 phone calls using dialers, 20–21, 118, 146–147  
 ping messages, 76  
 ping sweeps, 110–111, 324, 347  
 pop-up ads. *See also* Ad Blocking  
 blocking for specific accounts, 245  
 blocking with Web Assistant, 65  
 definition of, 16, 204  
 pop-up windows. *See* messages  
 port scans, 22–23, 110–111, 323, 347  
 ports  
 1900, rules blocking, 104  
 5000, rules blocking, 104  
 as back doors, 25  
 covert channeling attacks and, 324  
 definition of, 22  
 destination port, 345  
 list of, with corresponding applications, 75, 111  
 source port, 348  
 Post Office Protocol (POP), 282  
 Posum LLC, Task Lock program, 332–333  
 Practically Networked Web site, 232  
 Pre-Install Scanner, 48  
 Pretty Good Privacy (PGP)  
 encryption, 230, 331  
 Printer Spooler Service, 85  
 privacy  
 blocking private information sent online, 55–56, 218–219, 244–245, 264–265  
 children signing up for services, 335–336  
 cookies, blocking, 65, 215–216  
 cookies, deleting, 295–297  
 deleting temporary Internet files, 219  
 e-mail, employer's right to view, 200, 342  
 e-mail registrations, 190–191  
 History file, deleting, 220, 295–297  
 identity theft, 19–20, 26, 30  
 log files related to, 307–309  
 opting out of promotions or mailings, 341  
 preventing browser from sending information, 136–141, 217–220  
 private information alerts, 80  
 protecting, strategies for, 30, 341  
 shopping online and, 341  
 social engineering and, 26, 348  
 surfing anonymously, 191–192, 219, 333  
 Web Assistant and, 65  
 Privacy Control dialog box, 138–141, 216, 218, 244–245, 264–265  
*Privacy Journal* newsletter, 341  
 Privacy log, 308  
 PrivacyExchange Web site, 341  
 Privacy.Net Web site, 140  
 Private Information dialog box, 55  
 Private Information log, 308–309  
 private IP addresses, 74  
 private key, 331, 347  
 Product Activation dialog box, 53  
 product key, 49, 52–53  
 Productivity Control Wizard  
 creating accounts with, 242–243, 247–249  
 features of, 246–247  
 viewing and modifying account restrictions, 250  
 Professional version, features in, 298  
 Program Control  
 creating new location, 229–230  
 customizing Internet access, 88–92, 263–264  
 enabling and disabling, 92  
 running program scan, 86  
 viewing alert messages, 77–81  
 program scan, running, 85–91  
 programs. *See* applications  
 Protection, Norton, 290, 291–293  
 protocols, 23, 98. *See also specific protocols*  
 proxy server, problems with, 275–278  
 PSH (push) flag, 76  
 public key, 331, 348  
 public key cryptography, 348
- • •
- Quarantine area  
 definition of, 165–166, 348  
 errors in, 174  
 notification of files sent to, 167–168  
 properties of files in, 173  
 researching quarantined files, 168–170  
 restoring files from, 173  
 saving list of files in, 173  
 sending files to, 129–130, 166–167, 171, 175

Quarantine area (*continued*)  
 submitting quarantined files  
 to Symantec, 171–172  
 viewing and deleting items in,  
 130–131, 160–161

## • R •

RAM, 40, 67  
 RDS\_Shell attack, 94  
 Recycle Bin, 290–293  
 referrer information, tracked in  
 logs, 308  
 regedit command, 299  
 registration of Norton Internet  
 Security, 53, 285  
 registry  
 affected by manually  
 repairing viruses, 171  
 definition of, 43  
 removing Norton Internet  
 Security from, 299–300  
 Settings Alerts for, 79–80  
 remote access programs, 118  
 RemoteSpy program, 145  
 Repair Wizard, 129–130  
 Reports, Norton AntiVirus,  
 116–118, 130–131, 132  
 resources. *See also* Web sites  
 e-mail address for author, 7  
 mailing lists, 351–352  
 newsletters, 352  
 Symantec Security  
 Response, 28  
 Restricted User account, 247  
 Restricted Zone, 99  
 Restrictions log, 311  
 RnisUPG.exe program, 299  
 rootkits (hack tools), 118, 147  
 RST (reset) flag, 77  
 rule base, 348  
 rule-based crack, 20  
 rules  
 for Ad Blocking, 208–214  
 for application access, 88–91  
 blocking specific connections  
 from specific computers,  
 97–99  
 default, displaying and  
 modifying, 103–105  
 for packet filtering, 75–76  
 performance affected by,  
 155–156  
 priority of, setting, 105, 156

reviewing and modifying,  
 155–156  
 tracking rules being used,  
 317

## • S •

SANS (System Administration,  
 Networking and Security)  
 Institute, 350  
 Sarcnet.exe utility, 148  
 Sasser virus, 19  
 SaveNow program, 27  
 SC Magazine, 352  
 scams, e-mail, 26, 29–30, 336  
 Scan and Deliver Wizard,  
 171–172  
 screen saver password,  
 protecting, 334  
 ScreenLock Pro (iJen  
 Software), 334  
 Script Blocking feature, Norton  
 AntiVirus, 121–122  
 script kiddies, 18–19, 348  
 scripts, blocking, 121–122,  
 140–141, 214  
 search engines for children,  
 270  
 secure connections  
 inability to connect to secure  
 Web sites, 279–280  
 man-in-the-middle attacks  
 using, 323  
 using, 338–340  
 Secure Sockets Layer (SSL),  
 323, 338–340  
 Security Alerts, 79, 84, 138  
 Security Assistant Wizard, 85  
 security check  
 checking browser security,  
 136–138  
 scanning for viruses before  
 installation, 43–46  
 SecurityFocus HOME mailing  
 lists, 352  
 server, 348  
 services. *See also* applications  
 checking ports used by, 75  
 list of, with corresponding  
 ports and attacks, 23  
 performance affected by, 67  
 used by NIS, 280  
 Set Startup Account dialog  
 box, 58  
 Settings Alerts, 79–80

Shields UP! analysis tool, 227  
 Shoot The Messenger analysis  
 tool, 227  
 shopping online, security and,  
 341  
 shortcuts, removing, 300  
 signatures, attack  
 database of, 349  
 definition of, 93–94, 348  
 excluding from monitoring,  
 95–96  
 list of, detected by Norton  
 Personal Firewall, 94  
 tracked in log file, 307  
 updating, 58–60, 151–155  
 signatures, digital, 345  
 Smith, K. C. (spam merchant),  
 182  
 SMTP (Simple Mail Transfer  
 Protocol), 23, 282  
 SNMP (Simple Network  
 Management Protocol), 85  
 snmp.exe application, 85  
 social engineering, 26, 348  
 software. *See* applications  
 source port, 348  
 spam. *See also* Norton  
 AntiSpam  
 children receiving, 336  
 China as source of, 202  
 definition of, 16  
 on laptops, spam-blocking  
 software for, 228  
 MailWasher Pro for, 228, 332  
 recognizing, 183, 336  
 reducing, guidelines for, 183,  
 190–197  
 responding to, 183  
 sources of, 182–183  
 tracing source of, 201–202  
 SpamCop.net service, 200  
 Spector program, 145  
 SpectorPro software, 267  
 spiders, 182  
 spoofing  
 DNS, 346  
 IP, 25, 347  
 SpyChecker, Hijack This, 333  
 spyware  
 definition of, 26–27, 144–145  
 detecting, 327, 329–330  
 monitoring children's online  
 activity with, 266–267  
 SpywareInfo Web site, 327  
 SSL (Secure Sockets Layer),  
 323, 338–340

Standard User account, 247  
 startup account, choosing, 58, 248  
 static IP address, 24  
 station address, 73  
 Statistics window, 316–317  
 Stop Web Referral feature, 298  
 stores online, security and, 341  
 streaming, 13  
 subnet, blocking computers in, 97  
 subnet mask, 73  
 Supervisor account  
   creating, 241, 243, 247  
   password for, 238–240  
 support, 284, 285, 286–287  
 surfing anonymously, 191–192, 219, 333  
 Svchost.exe application, 84  
 Sygate Personal Firewall, 226  
 Symantec Event Manager, 85  
 Symantec Products and Services Web site, 11  
 Symantec Security Check, 111  
 Symantec Security Response  
   connecting to, 285  
   features of, 28, 349  
   newsletter from, 118  
   scanning for viruses before installation, 44–46  
   Search and Latest Virus Threats Web site, 169  
 Symantec Support page, 284, 285, 286–287  
 SYN floods, 322  
 SYN (synchronize) flag, 76  
 System Administration, Networking and Security (SANS) Institute, 350  
 System log, 311  
 system requirements, 40–41  
 System Restore  
   disabling before manual scan, 125  
   removing infected files from, 175–177  
   restoring files after wiping, 295  
 system tray, starting and stopping components from, 64–65  
 SystemWorks, Norton, 39

## • T •

Task Lock program (Posum LLC), 332–333  
 TCP (Transmission Control Protocol)  
   definition of, 23  
   firewall rules for, 76–77  
   Microsoft TCP/IP Configuration Utility, 85  
   tracking activity of, 317  
 Teenager account  
   application access restrictions for, 261–264  
   creating, 241, 243, 254–255  
   newsgroup access restrictions for, 261  
   Web site access restrictions for, 256–260  
 telephone calls using dialers, 20–21, 118, 146–147  
 temporary Internet files, deleting, 219  
 temporary IP address, 24  
 thieves, 19  
 Threat Alert log, 312  
 timeouts, preventing, 148–149  
 Transmission Control Protocol.  
   *See* TCP  
 Trojan horse. *See also* viruses  
   definition of, 25–26, 116, 325  
   manually repairing, 170–171  
 Trojan.Downloader.xxxx Trojan horse, 325  
 troubleshooting. *See also* alert messages; attacks; log files  
   Ad Blocking, problems with, 283–284  
   “always on” connections, problems with, 24  
   connections with network computers, losing, 101–105  
   e-mail, inability to send or receive, 282–283  
   installation of Norton Internet Security, problems with, 50–51  
   Norton AntiVirus, problems with, 174, 281–282  
   Norton Internet Security statistics, 316–317  
   performance, improving, 67, 155–156, 192, 204

proxy server, problems with, 275–278  
 resources for, 284–288  
 responding to problems, guidelines for, 273–274  
 secure Web sites, inability to connect to, 279–280  
 starting Norton Internet Security, problems with, 280–281  
 System Restore, infected files restored by, 175–177  
 tracking attack signatures, 307  
 tracking blocked content, 309–311  
 tracking connections, 305–307  
 tracking firewall activity, 317  
 tracking network activity, 317  
 tracking Norton AntiVirus activity, 311–312  
 tracking Norton Internet Security activity, 311  
 tracking privacy threats, 307–309  
 uninstalling and reinstalling Norton Internet Security, 174, 299–301  
 virus definitions corrupted, 174  
 Web sites, inability to connect to, 274–280  
 TRUSTe organization, 341  
 2003 Computer Crime and Security Survey, 17  
 2003 Virus Prevalence Survey, 60

## • U •

UDP (User Datagram Protocol), 23, 76, 81, 317  
 under ads, 204  
 UnErase Wizard, 291–293  
 Uniform Resource Locator (URL), 6, 205  
 unwanted content. *See* pop-up ads; spam  
 URG (urgent) flag, 77  
 Urgent Attention message, 63  
 URL (Uniform Resource Locator), 6, 205  
 users. *See* accounts, NIS

## • V •

virtual private network (VPN), 233

virus alerts, responding to, 128–131

virus definitions  
corrupted, 174  
downloading, 28  
updating, 58–60, 151–155

viruses. *See also* expanded threats; Norton AntiVirus; Trojan horse  
analysis tool for, 28  
anti-virus software for laptops, 227  
anti-virus software, Trojan horse posing as, 25  
on cellphones, 231  
definition of, 14–15, 115–116  
in downloaded software, 26–27  
examples of, 133  
in infected files, 27–28  
latest, viewing list of, 116–118  
macro virus, 27–28  
manually repairing, 170–171  
NIMDA virus, 23  
Online Virus Encyclopedia, viewing, 132  
quarantining, 129–131, 166–167, 171, 175  
repaired by Norton AntiVirus, 129  
reporting to Symantec, 131, 148  
researching, 168–170  
Sasser virus, 19  
scanning for, before installation, 43–46  
submitting to Symantec, 171–172  
threat report listing, 132  
tracked in log file, 312  
worms, 15, 116, 131, 324–325, 348

Visual Basic, blocking scripts using, 121–122, 140–141, 214

Visual Tracking, 106–107

Voice Over IP, 21

VPN (virtual private network), 233

## • W •

W32.Antinny.Q worm, 117

W32.Beagle worm, 325

W32.Gaobot.F0 worm, 117

W32.Korgo.D worm, 117

W32.Netsky worm, 324

W32.NetsupA@mm worm, 117

W32.Sasser worm, 325

war dialers, 20–21, 118, 146–147

Web Assistant toolbar, 65, 216

Web browser. *See* browser

Web Cleanup tool, 295–297

Web History log, 311. *See also* history of browser activity

Web sites  
addresses for, format used in this book, 6

Agnitum Outpost Firewall, 226

AmiWeb browser, 269

Anonymizer program, 192, 333

AntiVir Personal Edition, 227

AOL@School search engine, 270

Ask Jeeves search engine, 270

attack signatures, list of, 94

Automated Support Assistant, 287

Better Business Bureau, 341

Big Picture Book of Viruses, 14

blocked content, 140–141, 309–311

blocking ads based on, 209, 212–213

Bloodhound technology, 121

BumperCar browser, 269

CERT Coordination Center, 351

closing unintentional multiple windows created by, 298

Compelson Laboratories, 34

Convert Host Name to IP Address, 74

Cookie Crusher program, 332

Cookie Pal program, 332

CyberSleuth Kids search engine, 270

DShield, 109, 350

DSL Reports, 67

Electronic Privacy Information Center, 33

Emergency Disk program, 159–160

Encrypt-it! program, 232

Federal Trade Commission, 194

Firewall-Wizards mailing list, 352

FIRST, 351

For Dummies Web site, 7

Froogle, 228

Gibson Research Corporation, 227

Global Teck Web site, 231

Google Answers service, 288

GriSoft AVG Free Edition, 227

HFNetChk program, 338

Hijack This, 333

Homework Planet search engine, 270

HotSpotVPN service, 233

Hushmail service, 200

IamBigBrother software, 267

inability to connect to, 274–280

Incidents Web site, 350

Internet Assigned Numbers Authority, 75, 276

Internet Security Systems, 25

KaZaA, review of, 27

Kerio Personal Firewall, 226

Kevin Mitnick talk on social engineering, 26

KidRocket browser, 269

KidsBrowser browser, 269

KidsClick! search engine, 270

KidsWeb search engine, 270

Mail Preference Service, 194

MailWasher Pro, 228, 332

Microsoft Windows analysis tools, 227

Norton SystemWorks, 39

NTBugtraq mailing list, 351

PasswordSafe service, 33

PC Magazine, password manager review, 35

PDA Defense, 232

permitting access to, for specific accounts, 257–260

Practically Networked, 232

Pretty Good Privacy encryption, 331

PrivacyExchange, 341

Privacy.Net, 140

RemoteSpy program, 145

- removal utility for Norton Internet Security, 43, 51
  - restricting access to, for specific accounts, 250, 256–260
  - SANS Institute, 350
  - SC Magazine, 352
  - secure, inability to connect to, 279–280
  - security settings for, checking, 278–279
  - SecurityFocus HOME mailing lists, 352
  - Shields UP! analysis tool, 227
  - SpamCop.net service, 200
  - Spector program, 145
  - SpectorPro software, 267
  - SpywareInfo, 327
  - surfing anonymously, 191–192, 219, 333
  - Sygate Personal Firewall, 226
  - Symantec Products and Services, 11
  - Symantec Security Check, 111
  - Symantec Security Response, 45, 349
  - Symantec Security Response newsletter, 118
  - Symantec Security Response Search and Latest Virus Threats, 169
  - Symantec Support page, 284, 286–287
  - system requirements, 40–41
  - Task Lock program, 333
  - TRUSTe organization, 341
  - 2003 Computer Crime and Security Survey, 17
  - 2003 Virus Prevalence Survey, 60
  - Whitehats Network Security Response, 349
  - WHOIS search, 108
  - Yahooligans! News, 257
  - Yahooligans! search engine, 270
  - Zone Alarm, 226
  - “white hat” hackers, 18
  - Whitehats Network Security Response, 349
  - WHOIS search, 108–109
  - Windows Explorer, displaying Norton AntiVirus toolbar in, 66
  - Windows Internet Connection Firewall, disabling, 47, 274–275
  - Windows Registry. *See* registry
  - Windows Update, 330, 338
  - Windows Update Wizard, 229
  - winipcfg command, 75
  - Wipe Info window, 293–295
  - Wired Equivalent Privacy (WEP) encryption, 232
  - Wireless Home Networking For Dummies* (Briere; Hurley; Bruce), 233
  - wireless networks, 232–233
  - Wireless Networks For Dummies* (Davis; Lewis), 233
  - Word files, scanning, 143–144
  - worms. *See also* viruses
    - definition of, 15, 116, 324–325, 348
    - malicious worm alerts, 131
- X •
- XML (eXtensible Markup Language), used by ads, 205
- Y •
- Yahooligans! News Web site, 257
- Yahooligans! search engine, 270
- Yahoo!Mail, free e-mail address provided by, 192
- Yahoo!Messenger, 123–124
- Z •
- Zone Alarm, 226

