INDEX

Numerics

128-bit WEP, 30

64-bit WEP, 30

A

access control issues, troubleshooting, 22

access settings, verifying on ZoneAlarm, 14-15

account verification phishing scams, example of, 150

activating restore points, 88-90

active scanning mode (Windows Defender), 112

active scans, 59
- performing, 67
- scan options, configuring, 67–69

activity loggers, 138-141

Ad-Aware, 107

ad-hoc networking, disabling, 31, 48–50

Add/Remove Progams panel (Windows), removing spyware/adware, 114-115

advertising, eyeballs, 97

adware, 97
- “cow pattie” model, 99
- antiadware programs
  - *free versions, 103-107*
  - *installing, 102*
- as viruses, 99
- avoiding, 100
- infection, symptoms of, 113
- popup blocker (IE)
  - *enabling, 100*
  - *third-party, installing, 100-101*
- preventing, 99
- removing, 113
  - *with Add/Remove Programs panel, 114-115*
- uninstalling, 20–22
- Windows Defender, 70

AES (Advanced Encryption Standard), 29

always-on connections, 3

annoyware, 97

antispyware/antiadware programs
- as security bundle application, 112
- free versions, 103-107
- installing, 102

antivirus software, 59
- active scans, performing, 67
- components of, 59
- enabling with service provider, 62-63
- installing, 63–65
- scan options, configuring, 67-69
- selecting deployment locations, 61
- signatures, updating, 69
- virus detection, 60
- virus scans, performing, 65-67
- Windows Live OneCare, 70-71

applications, updating, 83-84

auto-update, 59

automatic operating system updates, enabling, 80-81

automatic signature updates, 69

avoiding
- phishing scams, 149-152
- spyware/adware, 100
- virus infection, 58-59

awareness of online dangers, instilling, 122-123

B

backing up files, 163-165
- destination, selecting, 166, 175-176
- frequency of, determining, 166
- using DVD/CD storage storage, 173
- using external hard drives, 168
- using Flash drives, 167
- using network storage drives, 169
- using online storage, 170, 173
- using Windows XP Backup, 176

banner ads, 97

blog sites, monitoring content of, 124-126

Bloodhound feature (Symantec), 68

bot armies, 4

browsers (IE), enabling popup blocker, 100

brute-force attacks, 3, 157

built-in firewalls, enabling, 8-9

built-in parental controls, 128-130
- on home computer, 134, 137
- on home network routers, 130-132

C

CD/DVD storage, 173

charities and phishing scams, 151

chat rooms versus IM, 122

comparing
- signature-based and heuristic virus detection, 61
- weak and strong passwords, 157-159

complacency as security threat, 187

components of antivirus software, 59

computer viruses. ***See*** **viruses**

configuring antivirus software, scan options, 67-69

contests prizes, phishing scam example, 151

"cow pattie" model, 99

Crack, 157

creating

- effective passwords, 157, 160-161
- restore points, 86-88
- strong passwords, 159-160

critical files, 165

D

data miners, 98

DDoS (distributed denial-of-service) attacks, 4

dedicated firewall devices, 9

default router passwords, changing, 31

destination, selecting for file backups, 166, 175-176

detecting

- malicious programs, 20-22
- viruses
  - *heuristic detection, 61*
  - *time-zero, 60*

disabling ad-hoc networking, 31, 48-50

disk scans

- active scans, 67
- performing, 65-67

drive-by downloads, 98

DVD storage, 173

E

effective passwords

- creating, 157-161
- elements of, 159

email

- phishing scams, 146
  - *avoiding, 149-152*
- pump-and-dump scams, 182-183
- worms, 56-57

enabling

- antispyware/antiadware in security bundles, 112
- antivirus software with ISP, 62-63
- automatic operating-system updates, 80-81
- built-in firewalls, 8-9
- encryption, 28
  - *WEP, 29, 33-36, 40-42*
  - *WPA, 29, 44-45*
- personal software firewalls, 10
  - *Windows XP firewall, 11-12*
  - *ZoneAlarm, 13*
- popup blocker on IE, 100

encryption

- troubleshooting, 48
- WEP, 29, 33
  - *enabling on wireless NIC, 35*
  - *enabling on wireless router, 33*
  - *enabling with Linksys WLAN Monitor, 36, 40*
  - *enabling with Windows XP, 40-42*
- WPA, enabling, 29, 44-45

encryption keys, generating, 30-31

encryption, enabling, 28

enforcing parental controls, 127-137

establishing Internet usage policy, 121-122

external hard drives, storing file backups, 168

eyeballs, 97

F

files, backing up, 163-165

- destination, selecting, 166, 175-176
- frequency of, determining, 166
- using DVD/CD storage, 173
- using external hard drives, 168
- using Flash drives, 167
- using network storage drives, 169
- using online storage, 170, 173
- using Windows XP Backup, 176

firewalls, 1

- access-control issues, troubleshooting, 22
- dedicated, 9
- deploying in home network, 8
- personal software, 6
  - *ZoneAlarm, 12-15*
  - *enabling, 10*
  - *McAfee Internet Security Suite, 18*
  - *selecting, 10, 16-18*
  - *Symantec Norton Internet Security 200x, 17*
  - *Windows XP firewall, 10-12*
- security scans, performing, 18-20
- SPI, 5-6

fixing corrupted operating systems, 90-92

Flash drives, storing file backups, 167

free antispyware/antiadware programs, 103-107

frequency of file backups, determining, 166

G-H

generating encryption keys, 30-31

- greed, role of in phishing scams, 151

guidelines for avoiding virus infection, 58-59

hard drives, storing file backups, 168

heuristic virus detection, 59-61

- Symantec Bloodhound feature, 68

hijackers, 98

home computers, enabling parental controls, 134, 137

home network routers, enabling controls, 130-132

"hot" merchandise scams, 184

I-J

IE (Internet Explorer), enabling popup blocker, 100

illegal peer-to-peer sharing, 120

IM (instant messaging) versus online chat rooms, 122

infected computers, repairing, 66, 72-74

installing
- antispyware/antiadware programs, 102
- antivirus software, 63-65
  - *selecting location for, 61*
- popup blockers, 100-101

Internet
- blog sites, monitoring, 125-126
- online dangers
  - *awareness of, instilling, 122-123*
  - *gambling, 119*
  - *hacking, 120*
  - *illegal peer-to-peer sharing, 120*
  - *pornography, 119*
  - *predators, 119*
  - *protecting children from, 120-121*
- parental controls, enforcing, 127-134, 137
- policing, 123-124
  - *with activity loggers, 138-141*
- usage policies, establishing, 121-122
- website history, monitoring, 126-127

ISPs
- antivirus software, enabling, 62-63
- built-in parental controls, 128-132

K-L

key generators, 30

key stroke loggers, 57

last known good, Windows restore points, 85-86
- activating, 88-90
- creating, 86-88

Lavasoft, Ad-Aware, 107

link redirects, phishing scams, 148-149

Linksys NSLU2, 170

Linksys WLAN Monitor, enabling WEP, 36, 40

Linksys WPC54GS Wireless-G PCMCIA laptop NIC, enabling WPA, 45

M

malicious programs, detecting, 20-22

manual operating system updates, performing, 82-83

McAfee Internet Security Suite, 18

mitigating security threats, tips for, 187-188

mnemonics, creating strong passwords, 159-160

money-exchange schemes, 183

monitoring children's Internet usage, 120-124
- activity loggers, 138-141
- blog sites, 125-126
- parental controls, 127-134, 137
- website history, 126-127

N-O

NAT (Network Address Translation), 8

NetNanny, 137

network storage drives, storing file backups, 169

Nigerian bank scams, 184

OneCare, 70-71

online activities
- parental controls, enforcing, 127-134, 137
- policing, 123-124
  - *with activity loggers, 138-141*

online chat rooms versus IM, 122

online dangers
- awareness of, instilling, 122-123
- gambling, 119
- hacking, 120
- illegal peer-to-peer sharing, 120
- Internet usage policy, establishing, 121-122
- pornography, 119
- predators, 119
- protecting children from, 120-122
- scams, protecting against, 182-185

online storage, 170, 173

operating systems
- automatic updates, enabling, 80-81
- manual updates, performing, 82-83
- repairing, 90-92
- restore points, 85-90
- updating, 79

P

parental controls
- built-in, 128, 130
- enforcing, 127-128
- on home computer, 134, 137
- on home network router, 130-132

passive scanning mode (Windows Defender), 110

password attacks, brute force, 3

passwords
- changing, 27, 161
- creating, 157
- effective, creating, 159-160
- on wireless routers, changing, 31
- securing, 160
- strong, anatomy of, 159
- weak, anatomy of, 157-159

peer-to-peer sharing, 120

performing
manual operating system updates, 82-83
security scans, 18-20
virus scans, 65-67
active scans, 67
scan options, configuring, 67-69
personal information, online security, 123
personal software firewalls, 5-6
access control, troubleshooting, 22
enabling, 10
McAfee Internet Security Suite, 18
security scans, performing, 18-20
selecting, 10, 16-18
Symantec Norton Internet Security 200x, 17
Windows XP firewall, 10
enabling, 11-12
ZoneAlarm, 12
access settings, verifying, 14-15
enabling, 13
logging facility, viewing, 16
phishing scams, 143, 145
account verification e-mail, example of, 150
avoiding, 149-152
nature of, 146
reporting, 153
tools used in, 146
types of, 150-151
phreaking, 145
policing children's Internet usage, 123-124
blog sites, monitoring, 125-126
parental controls
built-in, 128-130
enforcing, 127-128
on home computers, 134, 137
on home network router, 130-132
website history, monitoring, 126-127
with activity loggers, 138-139, 141
popup blockers, installing, 100-101
popups, 97
port-scanning utilities, performing security scans, 18-20
preventing
spyware/adware, 99
unintentional roaming, 50
viruses, 60-61
protecting children from online dangers, 120-123
Internet usage policy, establishing, 121-122
pump-and-dump scams, 182-183
purchasing, personal software firewalls, 16-18

Q-R

remote-control programs, 57
removing
malicious programs, 20-22
spyware/adware, 113
repairing
corrupted operating systems, 90-92
infected computers, 66, 72-74
reporting phishing scams, 153
restore points, 85-86
activating, 88-90
creating, 86-88
routers
built-in firewalls, enabling, 8-9
wireless, changing default password, 31

S

scams, protecting against, 182-185
scanning engines, 59
searchbars, 98
security bundles, 63
antispyware/antiadware programs, enabling, 112
security scans, performing, 18-20
Sedgewick, John, 187
selecting
antivirus software installation locations, 61
destination for file backups, 166, 175-176
personal software firewalls, 10, 16-18
Windows XP firewall, 10-12
ZoneAlarm, 12-15
SSIDs, 28
self-replication as characteristic of worms, 56-57
signatures, 59
active scans, performing, 67
detecting, 60
updating, 69
virus scans, performing, 65-67
social engineering, phishing scams, 143-145
avoiding, 149-152
nature of, 146
reporting, 153
tools used in, 146
software
security bundles, 135
updating, 83-84
Spare Backup, 171
SPI (stateful packet inspection) firewalls, 5-6
deploying in home network, 8
Spybot Search & Destroy, 103
automated scanning, 105-107
spyware, 97-98
"cow pattie" model, 99
antispyware programs
free versions, 103-107
installing, 102
as viruses, 99
avoiding, 100
infection, symptoms of, 113
popup blockers, installing, 100-101
preventing, 99

removal tools, 113
Add/Remove Programs panel, 114-115
Windows Defender, 70
SSIDs (service set identifiers), 25
changing, 32-33
selecting, 28
stocks, pump-and-dump scams, 182-183
storing file backups
CD/DVD storage, 173
on external hard drives, 168
on Flash memory, 167
on network storage drives, 169
online storage, 170, 173
strong passwords
anatomy of, 159
creating, 159-160
versus weak passwords, 157-159
Symantec, Bloodhound feature, 68
Symantec Norton Internet Security 200x, 17
symptoms of spyware/adware infection, 113
system files, 165-166

T

third-party popup blockers, installing, 100-101
threats, mitigating, 187-188
time-zero viruses, detecting, 60
tips
for creating strong passwords, 160-161
for mitigating security threats, 187-188
toolbars, 98
trackware, 98
Trojan horses, 57-58
troubleshooting
firewalls, access control issues, 22
wireless encryption, 48

U

uninstalling malicious programs, 20-22
unintentional roaming, preventing, 50
unsecured wireless networks, dangers of, 25
updating
antivirus software, need for, 79
operating system, 79
automatic updates, enabling, 80-81
manual updates, perfoming, 82-83
signatures, 69
software programs, 83-84
urban legends and home network security, 182
US-CERT (United States Computer Emergency Readiness Team), 79
user files, 165

V

verifying ZoneAlarm access settings, 14-15
viewing ZoneAlarm logging facility, 16
viruses, 55-56. *See also* antivirus software
heuristic detection, 61
infections
avoiding, 58-59
repairing, 72-74
preventing, 60-61
scanning for, 65-67
active scans, 67
scan options, configuring, 67-69
time-zero detecting, 60
visited-website history, monitoring, 126-127

W

war drivers, 25
warning boxes, 98
weak passwords, anatomy of, 157-159
websites
eyeballs, 97
link redirects, phishing scams, 146-149
uploaded content, monitoring, 124
WEP (Wired Equivalent Privacy), 29
enabling, 33
on wireless NIC, 35
on wireless routers, 33
with Linksys WLAN Monitor, 36, 40
with Windows XP, 40-42
Windows operating system. *See also* Windows XP
adware/spyware, removing with Add/Remove Progams panel, 114-115
repairing, 90
restore points, 85-86
activating, 88-90
creating, 86-88
Windows Defender, 70, 108-110
active scanning mode, 112
passive scanning mode, 110
Windows Live OneCare, 70-71
Windows XP
firewall, enabling, 11-12
System File Check utility, 92
WEP, enabling, 40-42
Windows XP Backup, 176
wireless network security, 25
ad-hoc networking, disabling, 31, 48-50
encryption
enabling, 28
troubleshooting, 48
WEP, 29, 33-36, 40-42
WPA, 29, 44-45
encryption keys, 30-31
implementing, 50

passwords, changing, 27
routers, changing default password, 31
SSID, changing, 28, 32-33
unintentional roaming, preventing, 50

work from home schemes, 183

worms, 56-57

WPA (Wi-Fi Protected Access), 29
enabling, 33, 44-45

X-Y-Z

ZoneAlarm, 12
access settings, enabling, 14-15
enabling, 13
logging facility, viewing, 16