

Contents at a Glance

<i>Introduction</i>	1
<i>Part I: Creating Your Own Homeland Security</i>	9
Chapter 1: Preparing Your Online Security Blanket	11
Chapter 2: Getting Started with Norton Internet Security	37
Chapter 3: Setting Rules for Your Firewall	69
Chapter 4: Strengthening and Customizing Your Firewall	93
<i>Part II: Handling Viruses and Malicious Code</i>	113
Chapter 5: Working with Norton AntiVirus	115
Chapter 6: Blocking Other Weapons of Mass Insecurity	135
Chapter 7: Performing Updates and Other Housekeeping	151
Chapter 8: Welcome to the Land of Quarantine	165
<i>Part III: Safeguarding Your Privacy and Your Network</i>	179
Chapter 9: Canning Spam	181
Chapter 10: Blocking Weapons of Mass Distraction	203
Chapter 11: Wireless and Laptop Security	221
<i>Part IV: Access Control</i>	235
Chapter 12: Issues for Networks with Multiple Users	237
Chapter 13: Issues for Young Users	251
<i>Part V: Getting Under the Hood</i>	271
Chapter 14: Troubleshooting	273
Chapter 15: This Old Computer: Housekeeping and Restoration	289
Chapter 16: Working With Log Files and Advanced Options	303
<i>Part VI: The Part of Tens</i>	319
Chapter 17: Ten Most Common Attacks	321
Chapter 18: Ten More Tools to Boost Your Privacy and Security	329
Chapter 19: Ten Security Threats NIS Doesn't Cover	335
<i>Part VII: Appendixes</i>	343
Appendix A: Glossary	345
Appendix B: Web Resources	349
<i>Index</i>	353

Table of Contents



<i>Introduction</i>	1
Yes, Virginia, You Can Find Safety and Privacy Online	1
How to Use This Book	2
Crazy Assumptions This Book Makes About You	2
How This Book Is Organized	3
Part I: Creating Your Own Homeland Security	3
Part II: Handling Viruses and Malicious Code	3
Part III: Safeguarding Your Privacy and Your Network	4
Part IV: Access Control	4
Part V: Getting under the Hood	5
Part VI: The Part of Tens	5
Part VII: Appendixes	5
Conventions Used in This Book	5
Icons Used in This Book	6
We're In It Together	7

Part I: Creating Your Own Homeland Security **9**

Chapter 1: Preparing Your Online Security Blanket **11**

Making the Case for Norton Internet Security	12
Erecting a firewall	12
Combating viruses	14
Blocking unwanted content	16
Keeping your business secure	17
Protecting your children	17
Understanding Hackers	18
“White Hat” hackers	18
Script kiddies	18
Thieves	19
Crackers	19
Demon dialers	20
What intruders want	21
Recognizing Garden-Variety Attacks	21
Port scans	22
IP address attacks	23
Back doors	25
Trojan horses	25
Social engineering: Ha, fooled ya!	26
Viruses in downloaded software	26
Infected files	27
Visiting Symantec Security Response	28



- Adopting Effective Privacy Strategies28
 - Don't believe everything you read29
 - Recognize suspicious e-mail warning signs29
 - Give out as little as possible30
- Managing Your Passwords31
 - Picking a good password31
 - Encrypting your passwords32

Chapter 2: Getting Started with Norton Internet Security 37

- Preparing Your Computer for Norton Internet Security37
 - Cleaning up your file system38
 - Doing a security check43
- Performing an Initial Virus Scan46
 - Preparing for installation48
 - Opening Norton Internet Security51
- Activating and Configuring NIS52
 - Handling post-installation tasks53
 - Detecting (or redetecting) the Internet60
- Using Norton Internet Security62
 - Touring the main window62
 - Starting or stopping components64
 - Setting options66

Chapter 3: Setting Rules for Your Firewall 69

- Understanding Your Firewall70
- Firewall Basics71
 - Positioning the firewall71
 - Guarding data transfer72
 - IP addressing for success73
 - Checking ports in a storm75
 - Filtering network traffic75
- Decoding All Those Alert Messages77
 - Categorizing alert messages78
 - Viewing alert details80
 - Investigating alerts with the Alert Assistant81
 - Disabling alert messages83
- Making Access Choices84
- What Do You Mean, That Program Is Trying to Access the Internet? ...85
- Running a Program Scan85
 - Automatic configuration88
 - Customizing Internet access88
- Unblocking Applications You Blocked92
- Turning Program Control On or Off92

Chapter 4: Strengthening and Customizing Your Firewall 93

- Working with Intrusion Detection93
 - Reducing intrusion alerts94
 - Deactivating intrusion detection96
 - Keeping a remote computer out of your network96

Configuring Your Network	101
Hello, computer! Identifying trusted machines	101
Tracking Down Hackers	105
Finding out about your attackers	105
Tracking hackers with WHOIS	108
Tracking hackers with DShield	109
Filing a report on your attacker	110
Ping sweeps and port scans	110
Deciding when to disable your firewall	111
Using Symantec Security Check	111

Part II: Handling Viruses and Malicious Code 113

Chapter 5: Working with Norton AntiVirus115

Recognizing Viruses and Their Notorious Relatives	115
Viewing the Newest Viruses	116
Identifying Expanded Threats	118
Configuring AntiVirus	119
Deciding how to respond	119
Protecting yourself from Internet threats	122
Running Your Own Virus Scan	124
Running a full system scan	125
Scanning selected files	126
Scheduling automatic virus scans	127
Responding to Virus Alerts	128
If the virus is repaired	129
If NAV can't repair or delete the file	129
If NAV places a file in Quarantine	130
If you see a malicious worm alert	131
Viewing Reports	132

Chapter 6: Blocking Other Weapons of Mass Insecurity135

Surfing the Web Safely	135
Blocking Web browser information	136
Working with compressed files	142
Protecting Microsoft Office Files	143
Keeping Spies and Hackers at Bay	144
Spyware	144
Keystroke loggers	145
Joke programs	146
Dialers	146
Hack tools	147
Handling Security Threats	147
Sending a file to Symantec over the Internet	148
Protecting against timeouts	148
Hitting the panic button	149

Chapter 7: Performing Updates and Other Housekeeping	151
Working with LiveUpdate	151
Running LiveUpdate	152
Reviewing Your Firewall Rules	155
Managing Passwords	157
Creating an Emergency Disk	158
From the CD	159
From the Symantec Web site	159
Housecleaning: Do You Really Need All This Stuff?	160
Cleaning out the Quarantine folder	160
Emptying Event logs	162
Chapter 8: Welcome to the Land of Quarantine	165
Quarantine Basics	165
Knowing when to quarantine a file	166
Researching quarantined data	167
Manually repairing viruses or Trojans	170
Working with Quarantine	171
Adding files to Quarantine	171
Submitting files with Scan and Deliver	171
Restoring files from Quarantine	173
Viewing Properties	173
Dealing with quarantine errors	174
Deleting original e-mail files	175
System Restore and Quarantine	175
 Part III: Safeguarding Your Privacy and Your Network	 179
Chapter 9: Canning Spam	181
The Web and Privacy: An Oxymoron	181
Where does spam come from?	182
Recognizing spam	183
Working with Norton AntiSpam	183
Changing default options	184
Training AntiSpam	186
Cutting Down on Spam	190
Reducing registrations	190
Anonymizing your browser	191
Creating a junk e-mail address	192
Opting to opt out	193
Canning Spam: More Approaches	194
Blocking addresses	194
Setting up filters	196

Practicing Safe E-Mail	197
Clearing your mail folders	198
Washing your e-mail	200
Concealing your e-mail address	200
Trying to trace your spammer	201
Chapter 10: Blocking Weapons of Mass Distraction	203
Halting Advertisements	203
Using Ad Blocking	204
Modifying how much Ad Blocking really blocks	210
Overriding block rules	210
Adding content to be blocked	212
Spitting Out Unwanted Cookies	214
Blocking cookies	215
Viewing cookie alerts	216
Keeping Your Web Activity Confidential	217
Adding or changing your private information	218
Deleting temporary Internet files	219
Chapter 11: Wireless and Laptop Security	221
Network Detector	221
Understanding Network Detector	222
Getting started with Network Detector	223
Laptop Security	225
Installing third-party security software	226
Securing your system	228
Creating a new location for your laptop	229
Using your laptop in a hotspot	230
Protecting your laptop from theft	230
Handheld Security	231
Protecting your cellphone	231
Protecting your PDA	232
Wireless Security	232
Obtaining an encryption key	232
Connecting to a Virtual Private Network	233
<i>Part IV: Access Control</i>	<i>235</i>
Chapter 12: Issues for Networks with Multiple Users	237
Understanding User Accounts	238
Default accounts	238
NIS accounts versus Windows accounts	240
Creating User Accounts	242
Creating accounts at startup	242
Creating accounts after startup	242
Logging on and off	244

Customizing User Accounts	244
Restricting Internet access	244
Boosting privacy	244
Blocking ads	245
Blocking spam	246
Managing Employees with Norton Productivity Control	246
Using the Productivity Control Wizard	247
Reviewing user restrictions	250

Chapter 13: Issues for Young Users251

Using Norton Parental Control	251
Enabling Parental Control	252
Identifying users	253
Reviewing the restricted list	256
Blocking newsgroups	261
Blocking applications	261
Blocking personal information	264
Viewing Web History	265
Spying on surfing activity	265
Monitoring other online activity	266
Password Protection	267
Password-protecting files and folders	267
Password-protecting your computer	268
Choosing Kid-Friendly Software	269
Web browsers	269
Search engines	270

Part V: Getting Under the Hood271

Chapter 14: Troubleshooting273

Unblocking Network Communications	274
You're unable to connect to a Web site	274
Problems starting up NIS	280
Problems with Individual Components	281
AntiVirus problems	281
Spam and e-mail weaknesses	282
Ad blocking problems	283
Finding Help	284
Exploring NIS's Help files	284
Trying context-sensitive help	286
Finding answers on the Web	286

Chapter 15: This Old Computer: Housekeeping and Restoration ..289

Obtaining the Norton Seal of Good Housekeeping	289
Protecting your Recycle Bin	290
Using Web Cleanup	295
Keeping your connection alive	297

Uninstalling and Reinstalling Norton Internet Security299
 Removing NIS from the Registry299
 Removing Symantec files, folders, and shortcuts300

Chapter 16: Working With Log Files and Advanced Options303

Viewing the Log Files304
 Tracking connections305
 Evaluating privacy threats307
 Reviewing blocked content309
 Keeping records of NIS’s activity311
 Using the AntiVirus Activity Log311
 Working with the Log Files312
 Refreshing log files313
 Saving log files313
 Disabling log records314
 Customizing Log Files314
 Changing log file size314
 Adjusting display settings315
 Advanced Options316
 Internet Connections317

***Part VI: The Part of Tens*319**

Chapter 17: Ten Most Common Attacks321

Denial of Service Attacks321
 SYN Floods322
 Invalid Packets322
 Port Scans323
 Man-in-the-Middle323
 Covert Channeling324
 Worms324
 Trojan Horses325
 Blended Threats326
 Browser Hijackers326

Chapter 18: Ten More Tools to Boost Your Privacy and Security . . .329

Ad-Aware329
 Windows Update330
 Pretty Good Privacy331
 MailWasher Pro332
 Cookie Crusher332
 Task Lock332
 Anonymizer333
 Hijack This333
 Password Officer333
 ScreenLock Pro334

Chapter 19: Ten Security Threats NIS Doesn't Cover	335
Children Signing Up for Services	335
Deceptive E-Mail Messages	336
Weak or Nonexistent Passwords	337
Forgetting to Install Patches	338
Failing to Encrypt Personal Information	338
Turning Off the Firewall	340
Forgetting to Opt Out	341
Not Being Careful about Where You Shop	341
Disgruntled Employees	342
Misusing Company Resources	342
Part VII: Appendixes	343
Appendix A: Glossary	345
Appendix B: Web Resources	349
Viruses and Security Incidents	349
Symantec Security Response	349
Whitehats Network Security Resource	349
Incidents.org	350
Dshield.org	350
Security Organizations	350
SANS Institute	350
The CERT Coordination Center	351
FIRST	351
Newsletters and Mailing Lists	351
NTBugtraq	351
Firewall-Wizards mailing list	352
SecurityFocus HOME mailing lists	352
SC Magazine	352
Index	353