

Contents at a Glance

<i>Introduction</i>	1
<i>Part I: Understanding the Problem</i>	9
Chapter 1: Spam and Spyware: The Rampant Menace	11
Chapter 2: The Spyware Who Loved Me: Stopping Spyware in Its Tracks	37
Chapter 3: Understanding the Enemy: What Really Spawns Spam	53
<i>Part II: Justifying and Selecting Spam and Spyware Filters</i>	69
Chapter 4: Calculating ROI for Your Anti-Spam and Anti-Spyware Measures	71
Chapter 5: Developing the Battle Plans	89
Chapter 6: Evaluating Anti-Spam and Anti-Spyware Solutions	107
<i>Part III: Deploying Your Chosen Solution</i>	133
Chapter 7: Training Users and Support Staff	135
Chapter 8: Planning the Rollout	149
Chapter 9: Rolling Out to the Enterprise	177
Chapter 10: Supporting Users	193
<i>Part IV: Maintaining Your Defenses</i>	207
Chapter 11: Everyday Maintenance	209
Chapter 12: Handling Thorny Issues	219
Chapter 13: Defense in Depth: Providing Layers of Protection	251
<i>Part V: The Part of Tens</i>	267
Chapter 14: Ten Spam-Filtering Solutions for the Enterprise	269
Chapter 15: Ten Keys to Successful Spam Filtering	279
Chapter 16: Ten Spam-Related Issues Most Enterprises Face	287
Chapter 17: Ten Spyware-Filtering Solutions for Businesses	295
Chapter 18: Ten Online Resources for Resolving Spam and Spyware	307
Chapter 19: Ten Keys to Successful Spyware Filtering	313
<i>Appendix A: Spam and Spyware Filtering Project Plan</i>	321

Appendix B: Spam and Spyware
Filtering Project Requirements327

Appendix C: Glossary341

Index349

Table of Contents

.....

<i>Introduction</i>	1
About This Book	2
Why We Combined Spam and Spyware	2
How This Book Is Organized	3
Part I: Understanding the Problem	3
Part II: Justifying and Selecting Spam and Spyware Filters	3
Part III: Deploying Your Chosen Solution	4
Part IV: Maintaining Your Defenses	4
Part V: The Part of Tens	4
Conventions Used in This Book	5
Defining Spam, Spyware, and Malware	5
Foolish Assumptions	6
Icons Used in This Book	6
Where to Go from Here	7
And the Latest Breaking News.	8
Write to Us!	8

Part I: Understanding the Problem **9**

Chapter 1: Spam and Spyware: The Rampant Menace	11
Knowing How Spam and Spyware Affect the Organization	11
Increasing e-mail volume	12
Draining productivity	12
Exposing the business to malicious code	14
Creating legal liabilities	14
No Silver Bullets: Looking for Ways to Fight Back	16
Adding a spam blocker	16
Keeping spyware away from workstations	20
Other good defense-in-depth practices	21
Understanding the role of legislation	21
Taking Stock of Your Business	22
Talk with people	22
Conduct a survey	23
Understanding your architecture	24
Taking users' skills and attitudes into account	25
Evaluating available skills in IT	26
Working within your budget	26
Justifying Spam and Spyware Control	27



- Choosing Anti-Spam and Anti-Spyware Solutions28
 - Types of anti-spam solutions29
 - What are the key features?30
 - Choosing the right model30
 - Sizing for now and the future32
- Making the Solution Work32
 - Creating a good plan33
 - Setting up a trial33
 - Training users35
 - Taking your solution live36
 - Maintaining the system36

Chapter 2: The Spyware Who Loved Me:

Stopping Spyware in Its Tracks 37

- What Is Spyware?37
 - An information collector38
 - An information transgressor38
- How Spyware Gets In40
 - Finding holes in the Web browser40
 - Tagging along in e-mail41
 - Hiding in software downloads41
 - Peer-to-peer file sharing42
- How Spyware Gets Information from Your Computer42
 - Hijacking cookies43
 - Executing programs43
 - Reading the Clipboard44
 - Accessing the hard drive44
 - Spoofing well-known Web pages44
 - Logging keystrokes45
- Fighting Back45
 - Testing for vulnerabilities45
 - Patching vulnerabilities46
 - Scanning and removing spyware47
 - Preventing spyware from getting a foothold48
- Choosing and Using Spyware Blockers49
 - Understanding the changing market49
 - Training users and getting their help50
 - Finding a product that deploys easily51
 - Using spyware blockers52

Chapter 3: Understanding the Enemy:

What Really Spawns Spam 53

- Understanding How Spammers Get E-Mail Addresses53
 - Harvesting from the Internet54
 - Buying and stealing addresses55
 - Directory service attacks56

Giving Filters the Slip: How Spam Messages Seep into Your Inbox58
 Poisoning Bayesian filters59
 Hash busting60
 Snowflaking messages61
 Forging From: and Received: headers61
 Relaying to hide message origins62
 The Economics of Spam64
 Making money with spam e-mail65
 A black market of bots for relaying spam65
 Spam’s New Attitude: The Convergence of Spam and Viruses66
 Advancing the War to New Fronts:
 Instant Messages and Text Messages67

***Part II: Justifying and Selecting
 Spam and Spyware Filters69***

**Chapter 4: Calculating ROI for Your Anti-Spam
 and Anti-Spyware Measures71**

Understanding Activity-Based Costing73
 Helpdesk example73
 Cost-of-e-mail example74
 As simple as ABC?75
 Understanding Fixed and Variable Costs75
 Volume-of-E-Mail Model76
 Using industry statistics76
 Surveying your users77
 Estimating your e-mail costs77
 Employee-Productivity Model79
 Estimating wasted time79
 Turning hours into dollars80
 Additional support calls because of spam
 and spyware-induced problems81
 Risk-Avoidance Model81
 Risks from chronic exposure to obscene,
 violent, and hate material82
 Risks from Web-site-borne malicious code82
 Risks from phishing scams83
 Qualitative Justifications84
 Executive frustration84
 Employee grumblings85
 Learning through networking85
 Models for Justifying Spyware Filters85
 Helpdesk support calls86
 Potential loss of corporate information86
 Potential loss of custodial data87
 Potential loss of employees’ private information87

Chapter 5: Developing the Battle Plans	89
Assessing Your Situation	89
Knowing thy present architecture	90
Knowing thy bandwidth	92
Knowing Your Business Objectives	93
Developing Requirements	94
What is a requirement?	94
Collecting and organizing requirements	96
Functional requirements	96
Technical requirements	97
Business requirements	98
Developing or Updating Policy	101
Re-Engineering Business Processes	102
Managing user accounts	102
Managing user workstations	102
Helpdesk	103
End-user training and orientation	103
E-mail administration	104
Network management	104
Managing the data center	104
Defining Roles and Responsibilities	105
Chapter 6: Evaluating Anti-Spam and Anti-Spyware Solutions . . .	107
Ensuring the Anti-Spam Cure Is Better Than the Original Spam	107
Choosing a Spam-Filtering Platform: Software, Appliance, or ASP?	109
Software solution	110
Appliance solution	112
Application Service Provider solution	113
Client-side solution	116
The solutions side-by-side	117
Choosing Spyware Filtering: Workstation or Centralized?	119
Workstation solutions	120
Centralizing the anti-spyware solution	120
Hybrid solutions	122
Evaluating Information from Vendors	123
Don't believe everything you hear	124
Calling customer references	125
Visiting a vendor's customer on-site	126
Visiting vendor sites	127
Other ways to obtain vendor information	128
Evaluating Anti-Spam and Anti-Spyware Vendors	129
Understanding vendors' long-term product strategies	129
Twisting vendors' arms to get the deal	131

***Part III: Deploying Your Chosen Solution* 133**
Chapter 7: Training Users and Support Staff135

The Many Methods of Training	135
Offering effective seminars	136
Creating paper user guides	138
Posting user guides online	140
Training Users	141
Looking at the technology from a user's point of view	142
Explaining the filter to users	142
Training Administrators	144
Put yourself in administrators' shoes	145
Including practice in the training	145
Give slightly more than needed	146
Training the Helpdesk Staff	146
Anticipating user questions and issues	147
Building a knowledge base	148

Chapter 8: Planning the Rollout149

Sketching Out a Plan	150
Involving the right people	150
Planning for disaster	151
Keeping your objectives in mind	153
Scheduling	153
Allocating Resources	154
Whose time do you need?	155
Estimating time for key tasks	158
Money, money, money	159
Rounding up the hardware and software	160
Working with outside resources	160
Tracking Tasks	162
Putting Together a Spam Filter Trial	163
Developing measurable success criteria	164
Performing tests	165
Selecting users for a trial	170
Evaluating trial results	171
Incorporating lessons learned into your deployment plan	172
Planning a Spyware Filter Trial	173
Needed: Measurable tests and results	174
Identifying false positives	174
Users' chores	174
Nondisruptive browser use	175

Chapter 9: Rolling Out to the Enterprise	177
Implementing Spam Filtering	177
Installing a software solution	178
Plugging in a hardware solution	180
Cutting over an ASP solution	181
Taking care of the administrative details	181
Measuring early results	186
Implementing Spyware Filtering	187
Starting with a trial installation	187
Installing throughout your business	188
Creating backout plans in case something goes awry	189
Keeping Everything under Control	189
Early warning signs of trouble	190
Changing the plan in mid-sentence	191
Testy testers	192
Chapter 10: Supporting Users	193
Understanding Common Support Scenarios	194
Gathering information for support scenarios	194
Documenting support scenarios	197
Equipping Support Staff with Tools and Knowledge	197
Seeing what the user sees	198
Knowledge	201
Measuring the Support Effort	203
Tracking numbers of calls	203
Tracking types of calls	204
Tracking the effort required to solve problems	205
Part IV: Maintaining Your Defenses	207
Chapter 11: Everyday Maintenance	209
Managing Quarantines	210
Involving end-users	210
Administrative maintenance	211
Automating quarantine management	212
Managing Whitelists	214
Maintaining user whitelists	214
Maintaining systemwide whitelists	215
Managing Filter Rules	215
Avoid specific rules that solve specific problems	216
Monitor how effective specific rules are	217
Managing Updates	217
Updating filter rules	217
Updating the software (or engine)	218

Chapter 12: Handling Thorny Issues	219
Coping with Performance Issues	220
Dealing with interruptions in mail service	220
Law of Big Numbers	221
Dealing with loss of productivity from spyware infestation	221
Setting Realistic User Expectations	222
False negatives: “Your inbox won’t be spam free”	223
False positives: When good mail looks bad	226
Restricting Web browser configuration	230
Identifying and Handling Business Issues	231
Figuring out legal issues	231
Uprooting hidden costs	233
Preparing for ASP outages	234
Developing skills to support the spam filter	235
What about when spam actually works?	238
Supporting spyware filters and scanning	239
Stopping Deliberate Attacks	239
Block Web bugs and other malicious content	240
Don’t make yourself a target for Joe Jobs	243
Prevent spammers from verifying or listing e-mail addresses	243
Make the Web spiders starve	244
Viruses — don’t be part of the problem	245
Shut out the robot army	245
Educate users about spammy NDRs	247
Protect users from phishing scams	248
Be aware of single-target spyware	249
 Chapter 13: Defense in Depth: Providing Layers of Protection	 251
Understanding Defense in Depth	251
Deploying Security Patches	252
Patches eliminate vulnerabilities	253
Keeping pace with viruses and worms	253
Patching made easier with dedicated tools	254
Managing Anti-Everything	255
Antivirus	256
Anti-popup	258
Filtering incoming e-mail attachment extensions	258
Turning off VRFY on your e-mail server	259
Managing Firewalls	259
Intranet firewalls	259
Filtering inbound as well as outbound	260
Keeping One Eye on the Future	262
Watching the spam-filtering market as it matures	262
Emerging standards	264
Watching the maturing anti-spyware market	266

Part V: The Part of Tens267**Chapter 14: Ten Spam-Filtering Solutions for the Enterprise269**

Brightmail AntiSpam 6.0	270
Postini Perimeter Manager	271
CipherTrust IronMail	272
FrontBridge TrueProtect Message Management Suite	273
Trend Micro Spam Prevention Solution	274
McAfee SpamAssassin	274
Sophos PureMessage	275
Tumbleweed MailGate	276
Proofpoint Messaging Security Gateway	277
MailFrontier Gateway Server	278

Chapter 15: Ten Keys to Successful Spam Filtering279

Knowing Your Users	279
Knowing the Product	280
Matching the Product to the Users	281
Training Users and Admins	282
Preparing to Troubleshoot	282
Preparing a Backout Plan	283
Revisiting Your Policies	284
Creating a Global Whitelist	284
Testing the Solution	285
Monitoring after You Deploy	285
Epilogue: Reviewing Your Original Business Objectives	286

Chapter 16: Ten Spam-Related Issues Most Enterprises Face287

Users Don't Check Their Quarantines	287
Users Don't Manage Their Whitelists	288
Too Many Helpdesk Calls	288
Important Messages Lost or Delayed	289
The Filter Vendor Exited the Market	290
If your solution is an ASP	290
If your solution is in-house	290
Your Filter Is No Longer Effective	291
Spam That Makes It through the Filter Is Still a Liability	291
Mail Delivery Becomes More Complex	292
Your Internet Connection Seems Slow	293
My Company's Products Smell Like Spam (Or, I Work for Hormel)	294

Chapter 17: Ten Spyware-Filtering Solutions for Businesses295

Ad-Aware Professional SE	296
SpywareBlaster 3.2	297
SpyBot - Search & Destroy	298
eTrust PestPatrol Anti-Spyware	299
Norton AntiVirus 2005	300

McAfee Anti-Spyware Enterprise Edition Module	301
Panda Platinum Internet Security 2005	302
SpyHunter	303
Yahoo! Anti-Spy Toolbar	303
Microsoft Windows AntiSpyware	304
Chapter 18: Ten Online Resources for Resolving Spam and Spyware	307
The Spamhaus Project	307
Coalition Against Unsolicited Commercial Email (CAUCE)	308
Internet Privacy For Dummies	309
The SPAM-L Tracking Spam FAQ	309
Federal Trade Commission (FTC)	310
SpywareInfo	310
Spychecker	311
GetNetWise	311
ScamBusters.org	312
Anti-Phishing Working Group	312
Chapter 19: Ten Keys to Successful Spyware Filtering	313
Understanding the Problem	313
Educating Your Users	315
Updating Your Policies	315
Choosing Products Wisely	316
Planning the Installation Judiciously	317
Testing Your Solution Thoroughly	317
Equipping the Helpdesk	318
Monitoring after Implementation	319
Reporting to Management	319
Watching the Product Market	320
<i>Appendix A: Spam- and Spyware- Filtering Project Plan</i>	<i>321</i>
<i>Appendix B: Spam- and Spyware- Filtering Project Requirements</i>	<i>327</i>
Common Requirements	328
Spam-Specific Requirements	335
Spyware-Specific Requirements	338
<i>Appendix C: Glossary</i>	<i>341</i>
<i>Index</i>	<i>349</i>

