

CONTENTS

Preface	xix
Acknowledgements	xxiv
1 Introduction to Phishing	1
1.1 What is Phishing?	1
1.2 A Brief History of Phishing	2
1.3 The Costs to Society of Phishing	4
1.4 A Typical Phishing Attack	5
1.4.1 Phishing Example: America's Credit Unions	6
1.4.2 Phishing Example: PayPal	10
1.4.3 Making the Lure Convincing	12
1.4.4 Setting The Hook	18
1.4.5 Making the Hook Convincing	20
1.4.6 The Catch	22
1.4.7 Take-Down and Related Technologies	23
1.5 Evolution of Phishing	23
1.6 Case Study: Phishing on Froogle	24
1.7 Protecting Users from Phishing	28
References	29
	vii

2	Phishing Attacks: Information Flow and Chokepoints	31
2.1	Types of Phishing Attacks	32
2.1.1	Deceptive Phishing	32
2.1.2	Malware-Based Phishing	34
2.1.3	DNS-Based Phishing (“Pharming”)	35
2.1.4	Content-Injection Phishing	36
2.1.5	Man-in-the-Middle Phishing	36
2.1.6	Search Engine Phishing	37
2.2	Technology, Chokepoints, and Countermeasures	37
2.2.1	Step 0: Preventing a Phishing Attack Before It Begins	38
2.2.2	Step 1: Preventing Delivery of Phishing Payload	40
2.2.3	Step 2: Preventing or Disrupting a User Action	43
2.2.4	Steps 2 and 4: Prevent Navigation and Data Compromise	49
2.2.5	Step 3: Preventing Transmission of the Prompt	50
2.2.6	Step 4: Preventing Transmission of Confidential Information	52
2.2.7	Steps 4 and 6: Preventing Data Entry and Rendering It Useless	55
2.2.8	Step 5: Tracing Transmission of Compromised Credentials	57
2.2.9	Step 6: Interfering with the Use of Compromised Information	58
2.2.10	Step 7: Interfering with the Financial Benefit	62
	References	62
3	Spoofing and Countermeasures	65
3.1	Email Spoofing	65
3.1.1	Filtering	68
3.1.2	Whitelisting and Greylisting	70
3.1.3	Ani-spam Proposals	71
3.1.4	User Education	73
3.2	IP Spoofing	74
3.2.1	IP Traceback	75
3.2.2	IP Spoofing Prevention	78
3.2.3	Intradomain Spoofing	80
3.3	Homograph Attacks Using Unicode	81
3.3.1	Homograph Attacks	81
3.3.2	Similar Unicode String Generation	82
3.3.3	Methodology of Homograph Attack Detection	83

3.4	Simulated Browser Attack	89
3.4.1	Using the Illusion	93
3.4.2	Web Spoofing	94
3.4.3	SSL and Web Spoofing	96
3.4.4	Ensnaring the User	98
3.4.5	SpoofGuard Versus the Simulated Browser Attack	99
3.5	Case Study: Warning the User About Active Web Spoofing	101
	References	102
4	Pharming and Client Side Attacks	105
4.1	Malware	105
4.1.1	Viruses and Worms	106
4.1.2	Spyware	115
4.1.3	Adware	115
4.1.4	Browser Hijackers	115
4.1.5	Keyloggers	116
4.1.6	Trojan Horses	116
4.1.7	Rootkits	116
4.1.8	Session Hijackers	118
4.2	Malware Defense Strategies	118
4.2.1	Defense Against Worms and Viruses	118
4.2.2	Defense Against Spyware and Keyloggers	121
4.2.3	Defense Against Rootkits	121
4.3	Pharming	122
4.3.1	Overview of DNS	123
4.3.2	Role of DNS in Pharming	124
4.3.3	Defense Against Pharming	125
4.4	Case Study: Pharming with Appliances	126
4.4.1	A Different Phishing Strategy	127
4.4.2	The Spoof: A Home Pharming Appliance	128
4.4.3	Sustainability of Distribution in the Online Marketplace	131
4.4.4	Countermeasures	132
4.5	Case Study: Race-Pharming	133
4.5.1	Technical Description	134
4.5.2	Detection and Countermeasures	135
4.5.3	Contrast with DNS Pharming	136
	References	137

5	Status Quo Security Tools	139
5.1	An Overview of Anti-Spam Techniques	139
5.2	Public Key Cryptography and its Infrastructure	144
5.2.1	Public Key Encryption	145
5.2.2	Digital Signatures	146
5.2.3	Certificates & Certificate Authorities	147
5.2.4	Certificates	149
5.3	SSL Without a PKI	151
5.3.1	Modes of Authentication	152
5.3.2	The Handshaking Protocol	152
5.3.3	SSL in the Browser	155
5.4	Honeypots	159
5.4.1	Advantages and Disadvantages	161
5.4.2	Technical Details	162
5.4.3	Honeypots and the Security Process	166
5.4.4	Email Honeypots	168
5.4.5	Phishing Tools and Tactics	170
	References	172
6	Adding Context to Phishing Attacks: Spear Phishing	175
6.1	Overview of Context-Aware Phishing	175
6.2	Modeling Phishing Attacks	177
6.2.1	Stages of Context-Aware Attacks	182
6.2.2	Identity Linking	185
6.2.3	Analyzing the General Case	187
6.2.4	Analysis of One Example Attack	190
6.2.5	Defenses Against Our Example Attacks	190
6.3	Case Study: Automated Trawling for Public-Private Data	191
6.3.1	Mother's Maiden Name: Plan of Attack	193
6.3.2	Availability of Vital Information	193
6.3.3	Heuristics for MMN Discovery	194
6.3.4	Experimental Design	196
6.3.5	Assessing the Damage	196
6.3.6	Time and Space Heuristics	198
6.3.7	MMN Compromise in Suffixed Children	199
6.3.8	Other Ways to Derive Mother's Maiden Names	199

6.4	Case Study: Using Your Social Network Against You	202
6.4.1	Motivations of a Social Phishing Attack Experiment	203
6.4.2	Design Considerations	203
6.4.3	Data Mining	204
6.4.4	Performing the Attack	206
6.4.5	Results	207
6.4.6	Reactions Expressed in Experiment Blog	208
6.5	Case Study: Browser Recon Attacks	210
6.5.1	Who Cares Where I've Been?	210
6.5.2	Mining Your History	211
6.5.3	CSS to Mine History	216
6.5.4	Bookmarks	218
6.5.5	Various Uses for Browser-Recon	218
6.5.6	Protecting Against Browser Recon Attacks	218
6.6	Case Study: Using the Autofill Feature in Phishing	219
6.7	Case Study: Acoustic Keyboard Emanations	221
6.7.1	Previous Attacks of Acoustic Emanations	223
6.7.2	Description of Attack	223
6.7.3	Technical Details	226
6.7.4	Experiments	231
	References	237
7	Human-Centered Design Considerations	241
7.1	Introduction: The Human Context of Phishing and Online Security	241
7.1.1	Human Behavior	241
7.1.2	Browser and Security Protocol Issues in the Human Context	243
7.1.3	Overview of the HCI and Security Literature	246
7.2	Understanding and Designing for Users	247
7.2.1	Understanding Users and Security	248
7.2.2	Designing Usable Secure Systems	255
7.3	Mis-Education	260
7.3.1	How Does Learning Occur?	260
7.3.2	The Lessons	261
7.3.3	Learning to Be Phished	269
7.3.4	Solution Framework	271
	References	273

8	Passwords	277
8.1	Traditional Passwords	277
8.1.1	Cleartext Passwords	277
8.1.2	Password Recycling	278
8.1.3	Hashed Passwords	278
8.1.4	Brute Force Attacks	280
8.1.5	Dictionary Attacks	281
8.1.6	Time-Memory Tradeoffs	281
8.1.7	Salted Passwords	283
8.1.8	Eavesdropping	284
8.1.9	One-Time Passwords	285
8.1.10	Alternatives to Passwords	285
8.2	Case Study: Phishing in Germany	286
8.2.1	Comparison of Procedures	286
8.2.2	Recent Changes and New Challenges	286
8.3	Security Questions as Password Reset Mechanisms	290
8.3.1	Knowledge-Based Authentication	291
8.3.2	Security Properties of Life Questions	292
8.3.3	Protocols Using Life Questions	296
8.3.4	Example Systems	298
8.4	One-Time Password Tokens	301
8.4.1	OTPs as a Phishing Countermeasure	306
8.4.2	Advanced Concepts	306
	References	308
9	Mutual Authentication and Trusted Pathways	309
9.1	The Need for Reliable Mutual Authentication	309
9.1.1	Distinctions Between the Physical and Virtual World	310
9.1.2	The State of Current Mutual Authentication	311
9.2	Password Authenticated Key Exchange	312
9.2.1	A Comparison Between PAKE and SSL	312
9.2.2	An Example PAKE Protocol: SPEKE	313
9.2.3	Other PAKE Protocols and Some Augmented Variations	316
9.2.4	Doppelgänger Attacks on PAKE	317
9.3	Delayed Password Disclosure	318
9.3.1	DPD Security Guarantees	320
9.3.2	A DPD Protocol	323

9.4	Trusted Path: How To Find Trust in an Unscrupulous World	327
9.4.1	Trust on the World Wide Web	328
9.4.2	Trust Model: Extended Conventional Model	329
9.4.3	Trust Model: Xenophobia	333
9.4.4	Trust Model: Untrusted Local Computer	333
9.4.5	Trust Model: Untrusted Recipient	335
9.4.6	Usability Considerations	338
9.5	Dynamic Security Skins	339
9.5.1	Security Properties	340
9.5.2	Why Phishing Works	340
9.5.3	Dynamic Security Skins	341
9.5.4	User Interaction	349
9.5.5	Security Analysis	350
9.6	Browser Enhancements for Preventing Phishing	351
9.6.1	Goals for Anti-Phishing Techniques	353
9.6.2	Google Safe Browsing	354
9.6.3	Phoolproof Phishing Prevention	358
9.6.4	Final Design of the Two-Factor Authentication System	360
	References	364
10	Biometrics and Authentication	369
10.1	Biometrics	369
10.1.1	Fundamentals of Biometric Authentication	371
10.1.2	Biometrics and Cryptography	377
10.1.3	Biometrics and Phishing	382
10.1.4	Phishing Biometric Characteristics	384
10.2	Hardware Tokens for Authentication and Authorization	385
10.3	Trusted Computing Platforms and Secure Operating Systems	387
10.3.1	Protecting Against Information Harvesting	392
10.3.2	Protecting Against Information Snooping	398
10.3.3	Protecting Against Redirection	405
10.4	Secure Dongles and PDAs	407
10.4.1	The Promise and Problems of PKI	408
10.4.2	Smart Cards and USB Dongles to Mitigate Risk	409
10.4.3	PostPKI Design and Use	413
10.4.4	PostPKI Evaluation	416
10.4.5	New Applications and Directions	419

10.5	Cookies for Authentication	420
10.5.1	Cache-Cookie Memory Management	423
10.5.2	Cache-Cookie Memory	423
10.5.3	C-Memory	424
10.5.4	TTF-Based Cache Cookies	425
10.5.5	Schemes for User Identification and Authentication	425
10.5.6	Identifier Trees	427
10.5.7	Rolling-Pseudonym Scheme	429
10.5.8	Denial-of-Service Attacks	430
10.5.9	Secret Cache Cookies	431
10.5.10	Audit Mechanisms	432
10.5.11	Proprietary Identifier-Trees	433
10.5.12	Implementation	434
10.6	Lightweight Email Signatures	435
10.6.1	Cryptographic and System Preliminaries	438
10.6.2	Lightweight Email Signatures	439
10.6.3	Technology Adoption	444
10.6.4	Vulnerabilities	447
10.6.5	Experimental Results	449
	References	453
11	Making Takedown Difficult	461
11.1	Derection and Takedown	461
11.1.1	Avoiding Distributed Phishing Attacks- Overview	464
11.1.2	Collection of Candidate Phishing Emails	465
11.1.3	Classification of Phishing Emails	465
	References	467
12	Protecting Browser State	469
12.1	Client-Side Protection of Browser State	469
12.1.1	Same-Origin Principle	470
12.1.2	Protecting Cache	473
12.1.3	Protecting Visited Links	474

12.2	Server-Side Protection of Browser State	476
12.2.1	Goals	478
12.2.2	A Server-Side Solution	480
12.2.3	Pseudonyms	481
12.2.4	Translation Policies	485
12.2.5	Special Cases	486
12.2.6	Security Argument	486
12.2.7	Implementation Details	487
12.2.8	Pseudonyms and Translation	487
12.2.9	General Considerations	490
	References	491
13	Browser Toolbars	493
13.1	Browser-Based Anti-Phishing Tools	493
13.1.1	Information-Oriented Tools	494
13.1.2	Database-Oriented Tools	501
13.1.3	Domain-Oriented Tools	507
13.2	Do Browser Toolbars Actually Prevent Phishing?	514
13.2.1	Study Design	514
13.2.2	Results and Discussion	517
	References	521
14	Social Networks	523
14.1	The Role of Trust Online	524
14.2	Existing Solutions for Securing Trust Online	527
14.2.1	Reputation Systems and Social Networks	527
14.2.2	Third-Party Certifications	532
14.2.3	First-Party Assertions	534
14.2.4	Existing Solutions for Securing Trust Online	535
14.3	Case Study: “Net Trust”	535
14.3.1	Identity	538
14.3.2	The Buddy List	539
14.3.3	The Security Policy	542
14.3.4	The Rating System	542
14.3.5	The Reputation System	543
14.3.6	Privacy Considerations and Anonymity Models	546
14.3.7	Usability Study Results	546
14.4	The Risk of Social Networks	548
	References	549

15 Microsoft's Anti-Phishing Technologies and Tactics	551
15.1 Cutting the Bait: SmartScreen Detection of Email Spam and Scams	552
15.2 Cutting the Hook: Dynamic Protection Within the Web Browser	556
15.3 Prescriptive Guidance and Education for Users	560
15.4 Ongoing Collaboration, Education, and Innovation	561
References	562
16 Using S/MIME	563
16.1 Secure Electronic Mail: A Brief History	564
16.1.1 The Key Certification Problem	565
16.1.2 Sending Secure Email: Usability Concerns	567
16.1.3 The Need to Redirect Focus	568
16.2 Amazon.com's Experience with S/MIME	569
16.2.1 Survey Methodology	569
16.2.2 Awareness of Cryptographic Capabilities	570
16.2.3 Segmenting the Respondents	573
16.2.4 Appropriate Uses of Signing and Sealing	574
16.3 Signatures Without Sealing	574
16.3.1 Evaluating the Usability Impact of S/MIME-Signed Messages	576
16.3.2 Problems from the Field	582
16.4 Conclusions and Recommendations	586
16.4.1 Promote Incremental Deployment	587
16.4.2 Extending Security from the Walled Garden	588
16.4.3 S/MIME for Webmail	589
16.4.4 Improving the S/MIME Client	590
References	590
17 Experimental evaluation of attacks and countermeasures	595
17.1 Behavioral Studies	595
17.1.1 Targets of Behavioral Studies	596
17.1.2 Techniques of Behavioral Studies for Security	597
17.1.3 Strategic and Tactical Studies	599
17.2 Case Study: Attacking eBay Users with Queries	600
17.2.1 User-to-User Phishing on eBay	602
17.2.2 eBay Phishing Scenarios	608
17.2.3 Experiment Design	609
17.2.4 Methodology	615
17.3 Case Study: Signed Applets	618
17.3.1 Trusting Applets	618
17.3.2 Exploiting Applets' Abilities	619
17.3.3 Understanding the Potential Impact	621

17.4	Case Study: Ethically Studying Man in the Middle	622
17.4.1	Man-in-the-Middle and Phishing	623
17.4.2	Experiment: Design Goals and Theme	628
17.4.3	Experiment: Man-in the-Middle Technique Implementation	629
17.4.4	Experiment: Participant Preparation	632
17.4.5	Experiment: Phishing Delivery Method	634
17.4.6	Experiment: Debriefing	635
17.4.7	Preliminary Findings	635
17.5	Legal Considerations in Phishing Research	640
17.5.1	Specific Federal and State Laws	641
17.5.2	Contract Law: Business Terms of Use	651
17.5.3	Potential Tort Liability	652
17.5.4	The Scope of Risk	654
17.6	Case Study: Designing and Conducting Phishing Experiments	655
17.6.1	Ethics and Regulation	657
17.6.2	Phishing Experiments - Three Case Studies	661
17.6.3	Making It Look Like Phishing	665
17.6.4	Subject Reactions	666
17.6.5	The Issue of Timeliness	667
	References	668
18	Liability for Phishing	671
18.1	Impersonation	671
18.1.1	Anti-SPAM	671
18.1.2	Trademark	674
18.1.3	Copyright	674
18.2	Obtaining Personal Information	675
18.2.1	Fraudulent Access	675
18.2.2	Identity Theft	676
18.2.3	Wire Fraud	677
18.2.4	Pretexting	677
18.2.5	Unfair Trade Practice	678
18.2.6	Phishing-Specific Legislation	678
18.2.7	Theft	680
18.3	Exploiting Personal Information	680
18.3.1	Fraud	680
18.3.2	Identity Theft	681
18.3.3	Illegal Computer Access	682
18.3.4	Trespass to Chattels	682
	References	685

19 The Future	687
References	694
Index	695
About the Editors	700