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 Hook 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 Pringle 24
  1.7 Protecting Users from Phishing 28
      References vii
2 Phishing Attacks: Information Flow and Chokepoints

2.1 Types of Phishing Attacks
   2.1.1 Deceptive Phishing
   2.1.2 Malware-Based Phishing
   2.1.3 DNS-Based Phishing ("Pharming")
   2.1.4 Content-Injection Phishing
   2.1.5 Man-in-the-Middle Phishing
   2.1.6 Search Engine Phishing

2.2 Technology, Chokepoints, and Countermeasures
   2.2.1 Step 0: Preventing a Phishing Attack Before It Begins
   2.2.2 Step 1: Preventing Delivery of Phishing Payload
   2.2.3 Step 2: Preventing or Disrupting a User Action
   2.2.4 Steps 3 and 4: Prevent Navigation and Data Compromise
   2.2.5 Step 5: Preventing Transmission of the Prompt
   2.2.6 Step 6: Preventing Transmission of Confidential Information
   2.2.7 Steps 4 and 6: Preventing Data Entry and Rendering It Useless
   2.2.8 Step 5: Tracking Transmission of Compromised Credentials
   2.2.9 Step 6: Interfering with the Use of Compromised Information
   2.2.10 Step 7: Interfering with the Financial Benefit

References

3 Spoofing and Countermeasures

3.1 Email Spoofing
   3.1.1 Filtering
   3.1.2 Whitelisting and Greylisting
   3.1.3 Anti-spam Proposals
   3.1.4 User Education

3.2 IP Spoofing
   3.2.1 IP Traceback
   3.2.2 IP Spoofing Prevention
   3.2.3 Intradomain Spoofing

3.3 Homograph Attacks Using Unicode
   3.3.1 Homograph Attacks
   3.3.2 Similar Unicode String Generation
   3.3.3 Methodology of Homograph Attack Detection
4 Pharming and Client Side Attacks

4.1 Malware
4.1.1 Viruses and Worms
4.1.2 Spyware
4.1.3 Adware
4.1.4 Browser Hijackers
4.1.5 Keyloggers
4.1.6 Trojan Horses
4.1.7 Rootkits
4.1.8 Session Hijackers

4.2 Malware Defense Strategies
4.2.1 Defense Against Viruses and Worms
4.2.2 Defense Against Spyware and Keyloggers
4.2.3 Defense Against Rootkits

4.3 Pharming
4.3.1 Overview of DNS
4.3.2 Role of DNS in Pharming
4.3.3 Defense Against Pharming

4.4 Case Study: Pharming with Appliances
4.4.1 A Different Phishing Strategy
4.4.2 The Spoof: A Home Pharming Appliance
4.4.3 Sustainability of Distribution in the Online Marketplace
4.4.4 Countermeasures

4.5 Case Study: Race-Pharming
4.5.1 Technical Description
4.5.2 Detection and Countermeasures
4.5.3 Contrast with DNS Pharming

References
5 Status Quo Security Tools

5.1 An Overview of Anti-Spam Techniques
5.2 Public Key Cryptography and its Infrastructure
  5.2.1 Public Key Encryption
  5.2.2 Digital Signatures
  5.2.3 Certificates & Certificate Authorities
  5.2.4 Certificates

5.3 SSL Without a PKI
  5.3.1 Modes of Authentication
  5.3.2 The Handshaking Protocol
  5.3.3 SSL in the Browser

5.4 Honeypots
  5.4.1 Advantages and Disadvantages
  5.4.2 Technical Details
  5.4.3 Honeypots and the Security Process
  5.4.4 Email Honeypots
  5.4.5 Phishing Tools and Tactics

References

6 Adding Context to Phishing Attacks: Spear Phishing

6.1 Overview of Context-Aware Phishing
6.2 Modeling Phishing Attacks
  6.2.1 Stages of Context-Aware Attacks
  6.2.2 Identity Linking
  6.2.3 Analyzing the General Case
  6.2.4 Analysis of One Example Attack
  6.2.5 Defenses Against Our Example Attacks

6.3 Case Study: Automated Traveling for Public Private Data
  6.3.1 Mother’s Maiden Name: Plan of Attack
  6.3.2 Availability of Vital Information
  6.3.3 Heuristics for MMN Discovery
  6.3.4 Experimental Design
  6.3.5 Assessing the Damage
  6.3.6 Time and Space Heuristics
  6.3.7 MMN Compromise in Suffixede Children
  6.3.8 Other Ways to Derive Mother’s Maiden Names
6.4 Case Study: Using Your Social Network Against You  
6.4.1 Motivations of a Social Phishing Attack Experiment  
6.4.2 Design Considerations  
6.4.3 Data Mining  
6.4.4 Performing the Attack  
6.4.5 Results  
6.4.6 Reactions Expressed in Experiment Blog  
6.5 Case Study: Browser Recon Attacks  
6.5.1 Who Cares Where I’ve Been?  
6.5.2 Mining Your History  
6.5.3 CSS to Mine History  
6.5.4 Bookmarks  
6.5.5 Various Uses for Browser Recon  
6.5.6 Protecting Against Browser Recon Attacks  
6.6 Case Study: Using the Autofill Feature in Phishing  
6.7 Case Study: Acoustic Keyboard Emulations  
6.7.1 Previous Attacks of Acoustic Emulations  
6.7.2 Description of Attack  
6.7.3 Technical Details  
6.7.4 Experiments  
References  

7 Human-Centered Design Considerations  
7.1 Introduction: The Human Context of Phishing and Online Security  
7.1.1 Human Behavior  
7.1.2 Browser and Security Protocol Issues in the Human Context  
7.1.3 Overview of the HCI and Security Literature  
7.2 Understanding and Designing for Users  
7.2.1 Understanding Users and Security  
7.2.2 Designing Usable Secure Systems  
7.3 Mix-Education  
7.3.1 How Does Learning Occur?  
7.3.2 The Lessons  
7.3.3 Learning to Be Phished  
7.3.4 Solution Framework  
References
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 286
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 Doppelganger 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
9.4.1 Trust on the World Wide Web
9.4.2 Trust Model: Extended Conventional Model
9.4.3 Trust Model: Xenophobia
9.4.4 Trust Model: Untrusted Local Computer
9.4.5 Trust Model: Untrusted Recipient
9.4.6 Usability Considerations
9.5 Dynamic Security Skins
9.5.1 Security Properties
9.5.2 Why Phishing Works
9.5.3 Dynamic Security Skins
9.5.4 User Interaction
9.5.5 Security Analysis
9.6 Browser Enhancements for Preventing Phishing
9.6.1 Goals for Anti-Phishing Techniques
9.6.2 Google Safe Browsing
9.6.3 Phishproof Phishing Prevention
9.6.4 Final Design of the Two-Factor Authentication System
References

10 Biometrics and Authentication
10.1 Biometrics
10.1.1 Fundamentals of Biometric Authentication
10.1.2 Biometrics and Cryptography
10.1.3 Biometrics and Phishing
10.1.4 Phishing: Biometric Characteristics
10.2 Hardware Tokens for Authentication and Authorization
10.3 Trusted Computing Platforms and Secure Operating Systems
10.3.1 Protecting Against Information Harvesting
10.3.2 Protecting Against Information Snipping
10.3.3 Protecting Against Redirection
10.4 Secure Dongles and PDAs
10.4.1 The Promise and Problems of PKI
10.4.2 Smart Cards and USB Dongles to Mitigate Risk
10.4.3 PorKi Design and Use
10.4.4 PorKi Evaluation
10.4.5 New Applications and Directions

~369~

~369~
10.5 Cookies for Authentication
  10.5.1 Cache-Cookie Memory Management
  10.5.2 Cache-Cookie Memory
  10.5.3 C-Memory
  10.5.4 TIP-Based Cache Cookies
  10.5.5 Schemes for User Identification and Authentication
  10.5.6 Identifier Trees
  10.5.7 Rolling-Pseudonym Scheme
  10.5.8 Denial-of-Service Attacks
  10.5.9 Secret Cache Cookies
  10.5.10 Audit Mechanisms
  10.5.11 Proprietary Identifier-Trees
  10.5.12 Implementation

10.6 Lightweight Email Signatures
  10.6.1 Cryptographic and System Preliminaries
  10.6.2 Lightweight Email Signatures
  10.6.3 Technology Adoption
  10.6.4 Vulnerabilities
  10.6.5 Experimental Results

References

11 Making Takedown Difficult
  11.1 Detection and Takedown
    11.1.1 Avoiding Distributed Phishing Attacks—Overview
    11.1.2 Collection of Candidate Phishing Emails
    11.1.3 Classification of Phishing Emails

References

12 Protecting Browser State
  12.1 Client-Side Protection of Browser State
    12.1.1 Same-Origin Principle
    12.1.2 Protecting Cache
    12.1.3 Protecting Visited Links

References
13.2 Server-Side Protection of Browser State
13.2.1 Goals
13.2.2 A Server-Side Solution
13.2.3 Pseudonyms
13.2.4 Translation Policies
13.2.5 Special Cases
13.2.6 Security Argument
13.2.7 Implementation Details
13.2.8 Pseudonyms and Translation
13.2.9 General Considerations
References

13 Browser Toolbars
13.1 Browser-Based Anti-Phishing Tools
13.1.1 Information-Oriented Tools
13.1.2 Database-Oriented Tools
13.1.3 Domain-Oriented Tools
13.2 Do Browser Toolbars Actually Prevent Phishing?
13.2.1 Study Design
13.2.2 Results and Discussion
References

14 Social Networks
14.1 The Role of Trust Online
14.2 Existing Solutions for Securing Trust Online
14.2.1 Reputation Systems and Social Networks
14.2.2 Third-Party Certifications
14.2.3 First-Party Assertions
14.2.4 Existing Solutions for Securing Trust Online
14.3 Case Study: “Net Trust”
14.3.1 Identity
14.3.2 The Buddy List
14.3.3 The Security Policy
14.3.4 The Rating System
14.3.5 The Reputation System
14.3.6 Privacy Considerations and Anonymity Models
14.3.7 Usability Study Results
14.4 The Risk of Social Networks
References
15 Microsoft's Anti-Phishing Technologies and Tactics

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

16.1 Secure Electronic Mail: A Brief History 564
16.1.1 The Key Certification Problem 566
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 570
16.2.2 Awareness of Cryptographic Capabilities 570
16.2.3 Segregating 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 Wall to the 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

17.1 Behavioral Studies 593
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 619
17.3.2 Exploiting Applets’ Abilities 619
17.3.3 Understanding the Potential Impact 624
17.4 Case Study: Ethically Studying Man in the Middle
17.4.1 Man-in-the-Middle and Phishing
17.4.2 Experiment: Design Goals and Theme
17.4.3 Experiment: Man-in-the-Middle Technique Implementation
17.4.4 Experiment: Participant Preparation
17.4.5 Experiment: Phishing Delivery Method
17.4.6 Experiment: Debriefing
17.4.7 Preliminary Findings
17.5 Legal Considerations in Phishing Research
17.5.1 Specific Federal and State Laws
17.5.2 Contract Law: Business Terms of Use
17.5.3 Potential Tort Liability
17.5.4 The Scope of Risk
17.6 Case Study: Designing and Conducting Phishing Experiments
17.6.1 Ethics and Regulation
17.6.2 Phishing Experiments: Three Case Studies
17.6.3 Making It Look Like Phishing
17.6.4 Subject Reactions
17.6.5 The Issue of Timeliness
References

18 Liability for Phishing
18.1 Impersonation
18.1.1 Anti-SPAM
18.1.2 Trademark
18.1.3 Copyright
18.2 Obtaining Personal Information
18.2.1 Fraudulent Access
18.2.2 Identity Theft
18.2.3 Wire Fraud
18.2.4 Pretexting
18.2.5 Unfair Trade Practice
18.2.6 Phishing-Specific Legislation
18.2.7 Theft
18.3 Exploiting Personal Information
18.3.1 Fraud
18.3.2 Identity Theft
18.3.3 Illegal Computer Access
18.3.4 Trespass to Chattels
References
CONTENTS

19 The Future

References

Index

About the Editors

687

694

695

700