PHISHING AND COUNTERMEASURES: UNDERSTANDING THE INCREASING PROBLEM OF ELECTRONIC IDENTITY THEFT

Preface.

Acknowledgements.

1. Introduction to Phishing.

1.1 What is Phishing?

1.2 A Brief History of Phishing.

1.3 The Costs to Society of Phishing.

1.4 A Typical Phishing Attack.

1.4.1 Phishing Example: Americas Credit Unions.

1.4.2 Phishing Example: PayPal.

1.4.3 Making The Lure Convincing.

1.4.4 Setting The Hook.

1.4.5 Making The Hook Convincing.

1.4.6 The Catch.

1.4.7 Take-Down and Related Technologies.

1.5 Evolution of Phishing.

1.6 Case Study: Phishing on Froogle.

1.7 Protecting Users from Phishing.

References.


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 2 and 4: Prevent Navigation and Data Compromise.
2.2.5 Step 3: Preventing Transmission of the Prompt.
2.2.6 Step 4: Preventing Transmission of Confidential Information.
2.2.7 Steps 4 and 6: Preventing Data Entry and Rendering it Useless.
2.2.8 Step 5: Tracing 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.
3.4 Simulated Browser Attack.
3.4.1 Using the Illusion.

BUY ONLINE AT: http://www.itgovernance.co.uk/products/1248
3.4.2 Web Spoofing.
3.4.3 SSL and Webspoofing.
3.4.4 Ensnaring the User.
3.4.5 SpoofGuard Versus the Simulated Browser Attack.
3.5 Case Study: Warning the User About Active Web Spoofing.

References.

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 Worms and Viruses.
4.2.2 Defense Against Spyware and Keyloggers.
4.2.3 Defending Against Rootkits.
4.3 Pharming.
4.3.1 Overview of DNS.
4.3.2 Role of DNS in Pharming.
4.3.3 Defending 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.

BUY ONLINE AT: http://www.itgovernance.co.uk/products/1248
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.


5.1 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 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 Heustics.

6.3.7 MMN Compromise in Suffixed Children.

6.3.8 Other Ways to Derive Mothers 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 Emanations.
6.7.1 Previous Attacks of Acoustic Emanations.
6.7.2 Description of Attack.
6.7.3 Technical Details.
6.7.4 Experiments.

References.

7. Human-Centered Design Considerations.
7.1.1 Human Behavior.
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 Mis-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.
8.1 Traditional Passwords.

BUY ONLINE AT: http://www.itgovernance.co.uk/products/1248
8.1.1 Cleartext Passwords.
8.1.2 Password recycling.
8.1.3 Hashed Passwords.
8.1.4 Brute force attacks.
8.1.5 Dictionary Attacks.
8.1.6 Time-Memory Tradeoffs.
8.1.7 Salted Passwords.
8.1.8 Eavesdropping.
8.1.9 One-Time Passwords.
8.1.10 Alternatives to Passwords.
8.2 Case Study: Phishing in Germany.
8.2.1 Comparison of Procedures.
8.2.2 Recent Changes and New Challenges.
8.3 Security Questions as Password Reset Mechanisms.
8.3.1 Knowledge Based Authentication.
8.3.2 Security Properties of Life Questions.
8.3.3 Protocols Using Life Questions.
8.3.4 Example Systems.
8.4 One-Time Password Tokens.
8.4.1 OTPs as a Phishing Countermeasure.
8.4.2 Advanced Concepts.

References.

9.1 The Need for Reliable Mutual Authentication.
9.1.1 Distinctions Between The Physical and Virtual World.
9.1.2 The State of Current Mutual Authentication.
9.2 Password Authenticated Key Exchange.
9.2.1 A Comparison Between PAKE and SSL.
9.2.2 An Example PAKE Protocol: SPEKE.
9.2.3 Other PAKE Protocols and Some Augmented Variations.
9.2.4 Doppelganger Attacks on PAKE.
9.3 Delayed Password Disclosure.
9.3.1 DPD Security Guarantees.
9.3.2 A DPD Protocol.
9.4 Trusted Path: How To Find Trust in an Unscrupulous World.
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 Phoolproof Phishing Prevention.
9.6.4 Final Design of the Two-Factor Authentication System.
References.

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.
10.3.1 Protecting Against Information Harvesting.
10.3.2 Protecting Against Information Snooping.
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 PorKl Design and Use.
10.4.4 PorKl Evaluation.
10.4.5 New Applications and Directions.
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 TIF-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.

BUY ONLINE AT: http://www.itgovernance.co.uk/products/1248
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.

11.1 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.

12.1 Client-Side Protection of Browser State.
12.1.1 Same-Origin Principle.
12.1.2 Protecting Cache.
12.1.3 Protecting Visited Links.
12.2 Server-Side Protection of Browser State.
12.2.1 Goals.
12.2.2 A Server-Side Solution.
12.2.3 Pseudonyms.
12.2.4 Translation Policies.
12.2.5 Special Cases.
12.2.6 Security Argument.
12.2.7 Implementation Details.
12.2.8 Pseudonyms and Translation.
12.2.9 General Considerations.

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. Microsofts Anti-Phishing Technologies and Tactics.
15.1 Cutting The Bait: SmartScreen Detection of Email Spam and Scams.
15.2 Cutting The Hook: Dynamic Protection Within the Web Browser.
15.3 Prescriptive Guidance and Education for Users.
15.4 Ongoing Collaboration, Education and Innovation.

References.

16. Using S/MIME.

16.1 Secure Electronic Mail: A Brief History.
16.1.1 The Key Certification Problem.
16.1.2 Sending Secure Email: Usability Concerns.
16.1.3 The Need to Redirect Focus.
16.2 Amazon.com's Experience with S/MIME.
16.2.1 Survey Methodology.
16.2.2 Awareness of Cryptographic Capabilities.
16.2.3 Segmenting the Respondents.
16.2.4 Appropriate Uses of Signing and Sealing.
16.3 Signatures Without Sealing.
16.3.1 Evaluating the Usability Impact of S/MIME-Signed Messages.
16.3.2 Problems from the Field.
16.4 Conclusions and Recommendations.
16.4.1 Promote Incremental Deployment.
16.4.2 Extending Security from the Walled Garden.
16.4.3 S/MIME for Webmail.
16.4.4 Improving the S/MIME Client.

References.

17. Experimental evaluation of attacks and countermeasures.

17.1 Behavioral Studies.
17.1.1 Targets of Behavioral Studies.
17.1.2 Techniques of Behavioral Studies for Security.
17.1.3 Strategic and Tactical Studies.

17.2 Case Study: Attacking eBay Users with Queries.
17.2.1 User-to-User Phishing on eBay.
17.2.2 eBay Phishing Scenarios.
17.2.3 Experiment Design.
17.2.4 Methodology.

17.3 Case Study: Signed Applets.
17.3.1 Trusting Applets.
17.3.2 Exploiting Applets Abilities.
17.3.3 Understanding the Potential Impact.

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.


Index.

About the Editors.