

1. Record Nr.	UNINA9911019295503321
Titolo	Phishing and countermeasures : understanding the increasing problem of electronic identity theft / / edited by Markus Jakobsson, Steven Myers
Pubbl/distr/stampa	Hoboken, N.J., : Wiley-Interscience, c2007
ISBN	9786610821969 9781280821967 1280821965 9780470086100 0470086106 9780470086094 0470086092
Descrizione fisica	1 online resource (730 p.)
Altri autori (Persone)	JakobssonMarkus MyersSteven <1975->
Disciplina	364.16/3
Soggetti	Phishing Identity theft - Prevention Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Phishing and Countermeasures; CONTENTS; 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: America's 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 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 2 and 4: Prevent Navigation and Data Compromise

2.2.5 Step 3: Preventing Transmission of the Prompt2.2.6 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 Prevention3.2.3 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; 3.4.2 Web Spoofing; 3.4.3 SSL and Web Spoofing; 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 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 Keyloggers4.1.6 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 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

---

### Sommario/riassunto

Phishing and Counter-Measures discusses how and why phishing is a threat, and presents effective countermeasures. Showing you how phishing attacks have been mounting over the years, how to detect and prevent current as well as future attacks, this text focuses on corporations who supply the resources used by attackers. The authors subsequently deliberate on what action the government can take to respond to this situation and compare adequate versus inadequate countermeasures.

---