1.

Record Nr.	UNINA9910138873603321
Titolo	The death of the internet / / edited by Markus Jakobsson
Pubbl/distr/stampa	Hoboken [New Jersey] : , : John Wiley & Sons, , c2012 [Piscataqay, New Jersey] : , : IEEE Xplore, , [2012]
ISBN	1-118-31254-6 1-280-99841-5 9786613770028 1-118-31253-8 1-118-31255-4
Edizione	[1st ed.]
Descrizione fisica	1 online resource (387 p.)
Classificazione	COM053000
Altri autori (Persone)	JakobssonMarkus
Disciplina	005.8
Soggetti	Internet - Security measures Electronic commerce - Security measures Data protection Computer crimes
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	Foreword xv -- Preface xvii -- Is the Title of this Book a Joke? xix -- Acknowledgments xxi -- Contributors xxiii -- Part I The Problem -- 1 What Could Kill the Internet? And so What? 3 -- 2 It is About People 7 -- 2.1 Human and Social Issues 7 / Markus Jakobsson -- 2.1.1 Nigerian Scams 8 -- 2.1.2 Password Reuse 9 -- 2.1.3 Phishing 11 -- 2.2 Who are the Criminals? 13 / Igor Bulavko -- 2.2.1 Who are they? 13 -- 2.2.2 Where are they? 14 -- 2.2.3 Deep-Dive: Taking a Look at Ex-Soviet Hackers 14 -- 2.2.4 Let's try to Find Parallels in the World we Live in16 -- 2.2.5 Crime and Punishment? 16 -- 3 How Criminals Profit 19 -- 3.1 Online Advertising Fraud 20 / Nevena Vratonjic, Mohammad Hossein Manshaei, and Jean-PierreHubaux -- 3.1.1 Advertising on the Internet 20 -- 3.1.2 Exploits of Online Advertising Systems 23 -- 3.1.3 Click Fraud 25 -- 3.1.4 Malvertising: Spreading Malware via Ads 31 -- 3.1.5 Inflight Modification of Ad Traffic 32 -- 3.1.6 Adware: Unsolicited Software Ads 34 -- 3.1.7 Conclusion 35 -- 3.2 Toeing the Line: Legal

but Deceptive Service Offers 35 / Markus Jakobsson and Ruilin Zhu -- 3.2.1 How Does it Work? 36 -- 3.2.2 What do they Earn? 36 -- 3.3 Phishing and Some Related Attacks 38 / Markus Jakobsson and William Leddy -- 3.3.1 The Problem is the User 38 -- 3.3.2 Phishing 38 -- 3.3.3 Man-in-the-Middle 39 -- 3.3.4 Man-in-the-Browser 40 -- 3.3.5 New Attack: Man-in-the-Screen 41 -- 3.4 Malware: Current Outlook 42 -- Members of the BITS Security Working Group and staff leads GregRattray and Andrew Kennedy -- 3.4.1 Malware Evolution 42 -- 3.4.2 Malware Supply and Demand 48 -- 3.5 Monetization 53 / Markus Jakobsson -- 3.5.1 There is Money Everywhere 53 -- 4 How ThingsWork and Fail 57 -- 4.1 Online Advertising: With Secret Security 58 / Markus Jakobsson -- 4.1.1 What is a Click? 58 -- 4.1.2 How Secret Filters are Evaluated 60 -- 4.1.3 What do Fraudsters Know? 62 -- 4.2 Web Security Remediation Efforts 63 / Jeff Hodges and Andy Steingruebl.

4.2.1 Introduction 63 -- 4.2.2 The Multitude of Web Browser Security Mechanisms 64 -- 4.2.3 Where do we go from Here? 75 -- 4.3 Content-Sniffing XSS Attacks: XSS with Non-HTML Content75 / Juan Caballero, Adam Barth, and Dawn Song -- 4.3.1 Introduction 75 -- 4.3.2 Content-Sniffing XSS Attacks 77 -- 4.3.3 Defenses 84 -- 4.3.4 Conclusion 89 -- 4.4 Our Internet Infrastructure at Risk 89 / Garth Bruen -- 4.4.1 Introduction 89 -- 4.4.2 The Political Structure 90 -- 4.4.3 The Domain 92 -- 4.4.4 WHOIS: Ownership and Technical Records 94 -- 4.4.5 Registrars: Sponsors of Domain Names 96 -- 4.4.6 Registries: Sponsors of Domain Extensions 97 -- 4.4.7 CCTLDs: The Sovereign Domain Extensions 99 -- 4.4.8 ICANN: The Main Internet Policy Body 100 -- 4.4.9 Conclusion 102 -- 4.5 Social Spam 103 / Dimitar Nikolov and Filippo Menczer -- 4.5.1 Introduction 103 -- 4.5.2 Motivations for Spammers 105 -- 4.5.3 Case Study: Spam in the GiveALink Bookmarking System108 -- 4.5.4 Web Pollution 114 -- 4.5.5 The Changing Nature of Social Spam: Content Farms 116 -- 4.5.6 Conclusion 117 -- 4.6 Understanding CAPTCHAs and Their Weaknesses 117 / Elie Bursztein -- 4.6.1 What is a Captcha? 117 -- 4.6.2 Types of Captchas 118 -- 4.6.3 Evaluating Captcha Attack Effectiveness 118 -- 4.6.4 Design of Captchas 119 -- 4.6.5 Automated Attacks 124 -- 4.6.6 Crowd-Sourcing: Using Humans to Break Captchas 127 -- 4.7 Security Questions 131 / Ariel Rabkin -- 4.7.1 Overview 131 -- 4.7.2 Vulnerabilities 134 -- 4.7.3 Variants and Possible Defenses 138 -- 4.7.4 Conclusion 139 -- 4.8 Folk Models of Home Computer Security 140 / Rick Wash and Emilee Rader -- 4.8.1 The Relationship Between Folk Models and Security 140 -- 4.8.2 Folk Models of Viruses and Other Malware 142 -- 4.8.3 Folk Models of Hackers and Break-Ins 146 -- 4.8.4 Following Security Advice 149 -- 4.8.5 Lessons Learned 153 -- 4.9 Detecting and Defeating Interception Attacks Against SSL154 / Christopher Soghoian and Sid Stamm -- 4.9.1 Introduction 154.

4.9.2 Certificate Authorities and the Browser Vendors 155 -- 4.9.3 Big Brother in the Browser 157 -- 4.9.4 Compelled Assistance 158 -- 4.9.5 Surveillance Appliances 159 -- 4.9.6 Protecting Users 160 -- 4.9.7 Threat Model Analysis 163 -- 4.9.8 Related Work 166 -- 4.9.9 Conclusion 168 -- 5 The Mobile Problem 169 -- 5.1 Phishing on Mobile Devices 169 / Adrienne Porter Felt and David Wagner -- 5.1.1 The Mobile Phishing Threat 170 -- 5.1.2 Common Control Transfers 172 -- 5.1.3 Phishing Attacks 178 -- 5.1.4 Web Sender&#x21D2; Mobile Target 182 -- 5.1.5 Web Sender&#x21D2;Web Target 184 -- 5.1.6 Attack Prevention 185 -- 5.2 Why Mobile Malware will Explode 185 / Markus Jakobsson and Mark Grandcolas -- 5.2.1 Nineteen Eighty-Six: When it all Started 186 -- 5.2.2 A Glimpse of Users 186 -- 5.2.3 Why Market Size Matters 186 -- 5.2.4 Financial Trends 187 --

5.2.5 Mobile Malware Outlook 187 -- 5.3 Tapjacking: Stealing Clicks on Mobile Devices 189 / Gustav Rydstedt, Baptiste Gourdin, Elie Bursztein, and DanBoneh -- 5.3.1 Framing Attacks 189 -- 5.3.2 Phone Tapjacking 191 -- 5.3.3 Framing Facebook 194 -- 5.3.4 Summary and Recommendations 195 -- 6 The Internet and the PhysicalWorld 197 -- 6.1 Malware-Enabled Wireless Tracking Networks 197 / Nathaniel Husted and Steven Myers -- 6.1.1 Introduction 198 -- 6.1.2 The Anatomy of a Modern Smartphone 199 -- 6.1.3 Mobile Tracking Networks: A Threat to Smartphones 200 -- 6.1.4 Conclusion 219 -- 6.2 Social Networking Leaks 219 / Mayank Dhiman and Markus Jakobsson -- 6.2.1 Introduction 220 -- 6.2.2 Motivations for Using Social Networking Sites 220 -- 6.2.3 Trust and Privacy 221 -- 6.2.4 Known Issues 222 -- 6.2.5 Case Study: Social Networking Leaks in the Physical World225 -- 6.3 Abuse of Social Media and Political Manipulation 231 / Bruno Gond calves, Michael Conover, and FilippoMenczer -- 6.3.1 The Rise of Online Grassroots Political Movements 231 -- 6.3.2 Spam and Astroturfing 232 -- 6.3.3 Deceptive Tactics 233 -- 6.3.4 The Truthy System for Astroturf Detection 236.
6.3.5 Discussion 240 -- Part II Thinking About Solutions -- 7 Solutions to the Problem 245 -- 7.1 When and How to Authenticate 245 / Richard Chow, Elaine Shi, Markus Jakobsson, Philippe Golle,Ryusuke Masuoka, Jesus Molina, Yuan Niu, and Jeff Song -- 7.1.1 Problem Description 246 -- 7.1.2 Use Cases 247 -- 7.1.3 System Architecture 248 -- 7.1.4 User Privacy 250 -- 7.1.5 Machine Learning/Algorithms 250 -- 7.1.6 User Study 252 -- 7.2 Fastwords: Adapting Passwords to Constrained Keyboards255 / Markus Jakobsson and Ruj Akavipat -- 7.2.1 The Principles Behind Fastwords 256 -- 7.2.2 Basic Feature Set 258 -- 7.2.3 Extended Feature Set 260 -- 7.2.4 Sample Stories and Frequencies 261 -- 7.2.5 Recall Rates 262 -- 7.2.6 Security Analysis 264 -- 7.2.7 The Security of Passwords 264 -- 7.2.8 Entry Speed 268 -- 7.2.9 Implementation of Fastword Entry 270 -- 7.2.10 Conclusion 271 -- 7.3 Deriving PINs from Passwords 271 / Markus Jakobsson and Debin Liu -- 7.3.1 Introduction 272 -- 7.3.2 A Brief Discussion of Passwords 273 -- 7.3.3 How to Derive PINs from Passwords 274 -- 7.3.4 Analysis of Passwords and Derived PINs 275 -- 7.3.5 Security Analysis 278 -- 7.3.6 Usability Experiments 280 -- 7.4 Visual Preference Authentication 282 / Yuan Niu, Markus Jakobsson, Gustav Rydstedt, and DahnTamir -- 7.4.1 Password Resets 282 -- 7.4.2 Security Questions Aren't so Secure 283 -- 7.4.3 What is Visual Preference-Based Authentication 283 -- 7.4.4 Evaluating Visual Preference-Based Authentication 285 -- 7.4.5 Case Study: Visual Blue Moon Authentication 286 -- 7.4.6 Conclusion 290 -- 7.5 The Deadly Sins of Security User Interfaces 290 / Nathan Good -- 7.5.1 Security Applications with Frustrating User Interfaces291 -- 7.5.2 The Four Sins of Security Application User Interfaces293 -- 7.5.3 Consumer Choice: A Security Bugbear 293 -- 7.5.4 Security by Verbosity 299 -- 7.5.5 Walls of Checkboxes 300 -- 7.5.6 All or Nothing Switch 302 -- 7.5.7 Conclusion 304 -- 7.6 SpoofKiller-Let's Kiss Spoofing Goodbye!304 / Markus Jakobsson and William Leddy.
7.6.1 A Key to the Solution: Interrupts 305 -- 7.6.2 Why can the User Log in to Good Sites, but not Bad Ones?305 -- 7.6.3 What About Sites that are Good . . . but not CertifiedGood? 308 -- 7.6.4 SpoofKiller: Under the Hood 309 -- 7.6.5 Say we Implement SpoofKiller-then What? 311 -- 7.7 Device Identification and Intelligence 312 / Ori Eisen -- 7.7.1 1995-2001: The Early Years of Device Identification313 -- 7.7.2 2001-2008 Tagless Device Identification Begins314 -- 7.7.3 2008-Present: Private Browsing and Beyond 319 -- 7.8 How can we Determine if a Device is Infected or not?323 / Aur'elien Francillon,

Markus Jakobsson, and AdrianPerrig -- 7.8.1 Why Detection is Difficult 323 -- 7.8.2 Setting up an Isolated Environment 324 -- 7.8.3 What Could go Wrong? 326 -- 7.8.4 Brief Comparison with TrustZone 328 -- 7.8.5 Summary 328 -- 8 The Future 331 -- 8.1 Security Needs the Best User Experience 332 / Hampus Jakobsson -- 8.1.1 How the User Won Over Features 332 -- 8.1.2 So How Come the iPhone Became so Successful? 332 -- 8.1.3 A World of Information Anywhere 333 -- 8.1.4 Midas' Touch Screens 334 -- 8.1.5 New Input, New Opportunities 335 -- 8.1.6 Zero-Click and Real-Life User Interfaces 335 -- 8.1.7 Privacy and User Interfaces 336 -- 8.1.8 It all Comes Together 336 -- 8.2 Fraud and the Future 336 / Markus Jakobsson -- References 339 -- Index 359.

Sommario/riassunto

A holistic look at the vast landscape of Internetsecurity-past, present, and futureA major attack on the Internet could wreak havoc onsociety-bringing down telephony, banking, business,government, media, and the energy grid. This book addresses thegrowing threats to the Internet from different sources, offeringin-depth guidance on how to combat them on both desktop and mobileplatforms.Edited by a specialist in holistic security with contributionsfrom experts in industry and academia, The Death of theInternet presents a unique, cross-disciplinary approach toInternet security. It goes beyond computer science to explore itssocial and psychological components, discussing politicallymotivated attacks, human error, and criminal tendencies. Geared tonon-technical readers and experts alike, the book clearly explainsthe general concepts of Internet security for managers anddecision-makers and provides engineers and industry professionalswith detailed instructions on how to develop effective designs withsecurity in mind. The Death of the Internet:. Covers topics of Internet security, online fraud, phishing, andmalware. Explores the growing need for dedicated smartphone Internetsecurity. Describes how security threats can result in loss of trust andadvertising revenues. Outlines proven countermeasures and explains how to implementthem using real-world examples. Reviews state-of-the-art research and future trends in Internetsecurity.