Anti-Phishing Education App

Design, Implementation and EvaluationMaster-Thesis von Clemens Bergmann und Gamze Canova
Dezember 2013



Fachbereich Informatik Security, Usability and Society Anti-Phishing Education App Design, Implementation and Evaluation

Vorgelegte Master-Thesis von Clemens Bergmann und Gamze Canova

1. Gutachten: Professor Dr. Melanie Volkamer

2. Gutachten: Arne Renkema-Padmos

Tag der Einreichung:

Bitte zitieren Sie dieses Dokument als: URN: urn:nbn:de:tuda-tuprints-12345

URL: http://tuprints.ulb.tu-darmstadt.de/1234

Dieses Dokument wird bereitgestellt von tuprints, E-Publishing-Service der TU Darmstadt http://tuprints.ulb.tu-darmstadt.de tuprints@ulb.tu-darmstadt.de



Die Veröffentlichung steht unter folgender Creative Commons Lizenz: Namensnennung – Keine kommerzielle Nutzung – Keine Bearbeitung 2.0 Deutschland http://creativecommons.org/licenses/by-nc-nd/2.0/de/

Erklärung zur Master-Thesis

Hiermit versichere ich, die vorliegende Master-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 18. Dezember 2013	
(C. Bergmann)	-

Erklärung zur Master-Thesis

Hiermit versichere ich, die vorliegende Master-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 18. Dezember 2013	
(G. Canova)	-

Inhaltsverzeichnis

1	Introduction	1
	1.1 Motivation	1
		1
	1.1.3 Technical Solutions	
	1.1.4 Anti-Phishing Education on the Smartphone	
	1.2 Goals	
		1
	1.4 Outline	1
_	Da domestin d	4
2	Background 2.1 Definition of Phishing	1
	2.2 Phishing Techniques	
	2.3 Phishing Attack Channels	
	2.4 Variations of Phishing	
	2.5 Summary - Phishing in this Work	2
3	Related Work	2
		3
	3.2 Way of Communication	
	3.3 State of the Art	3
	3.4 Pro and Contra Discussion	Э
4	System Requirements, Assumptions and Limitations	3
	4.1 System Requirements	
	4.2 Assumptions	
	4.3 Limitations of Our Approach	3
_		
		_
5	Target Group	3
		3
6	Pre-Survey	3
		3
	Pre-Survey 6.1 Main Objective	3
6	Pre-Survey 6.1 Main Objective	3 4 4 4
	Pre-Survey 6.1 Main Objective	3 4 4 4
6	Pre-Survey 6.1 Main Objective	3 4 4 4 4 4
6	Pre-Survey 6.1 Main Objective	3 4 4 4 4 4 4
6	Pre-Survey 6.1 Main Objective	3 4 4 4 4 4 4
6	Pre-Survey 6.1 Main Objective 6.2 Survey Details 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization 7.2 Android Elements	3 4 4 4 4 4 4
6	Pre-Survey 6.1 Main Objective . 6.2 Survey Details . 6.3 Evaluation . Teaching and Learning Content 7.1 Phishing URLs . 7.1.1 Phishing URL Categorization . 7.1.2 Problems and Challenges With The Categorization . 7.1.2 Android Elements . 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing .	3 4 4 4 4 4 4 4 4
6	Pre-Survey 6.1 Main Objective 6.2 Survey Details 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization 7.1.3 Android Elements 7.1 Android Browser Security Indicators 7.4 E-Mail Spoofing 7.4.1 General Recommended Behavior	3 4 4 4 4 4 4 4 4
6	Pre-Survey 6.1 Main Objective . 6.2 Survey Details . 6.3 Evaluation . Teaching and Learning Content 7.1 Phishing URLs . 7.1.1 Phishing URL Categorization . 7.1.2 Problems and Challenges With The Categorization . 7.1.2 Android Elements . 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing .	3 4 4 4 4 4 4 5
7	Pre-Survey 6.1 Main Objective 6.2 Survey Details 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization 7.1 Android Elements 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing 7.4.1 General Recommended Behavior 7.5 Conclusion / Summary	3 4 4 4 4 4 5 5 5 5
6	Pre-Survey 6.1 Main Objective	3 4 4 4 4 4 4 5 5 5 5 5 5
7	Pre-Survey 6.1 Main Objective 6.2 Survey Details 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization 7.1 Android Elements 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing 7.4.1 General Recommended Behavior 7.5 Conclusion / Summary Approach for Our Anti-Phishing Education App 8.1 App Design	3 4 4 4 4 4 4 5 5 5 5 5
7	Pre-Survey 6.1 Main Objective . 6.2 Survey Details . 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs . 7.1.1 Phishing URL Categorization . 7.1.2 Problems and Challenges With The Categorization 7.1 Android Elements . 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing . 7.4.1 General Recommended Behavior 7.5 Conclusion / Summary . Approach for Our Anti-Phishing Education App 8.1 App Design . 8.2 Game Rules .	3 4 4 4 4 4 4 5 5 5 5 5 5 5
7	Pre-Survey 6.1 Main Objective . 6.2 Survey Details 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization 7.1.2 Problems Security Indicators 7.3 Android Elements 7.4 E-Mail Spoofing 7.4.1 General Recommended Behavior 7.5 Conclusion / Summary Approach for Our Anti-Phishing Education App 8.1 App Design 8.2 Game Rules 8.3 Leveling Strategy	3 4 4 4 4 4 4 5 5 5 5 5
7	Pre-Survey 6.1 Main Objective 6.2 Survey Details 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization 7.2 Android Elements 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing 7.4.1 General Recommended Behavior 7.5 Conclusion / Summary Approach for Our Anti-Phishing Education App 8.1 App Design 8.2 Game Rules 8.3 Leveling Strategy	3 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5
7	Pre-Survey 6.1 Main Objective . 6.2 Survey Details 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization 7.1.2 Android Elements 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing 7.4.1 General Recommended Behavior 7.5 Conclusion / Summary Approach for Our Anti-Phishing Education App 8.1 App Design 8.2 Game Rules 8.3 Leveling Strategy 8.4 Knowledge Transfer Per Level	3 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5
8	Pre-Survey 6.1 Main Objective 6.2 Survey Details 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization 7.1.3 Android Elements 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing 7.4.1 General Recommended Behavior 7.5 Conclusion / Summary Approach for Our Anti-Phishing Education App 8.1 App Design 8.2 Game Rules 8.3 Leveling Strategy 8.4 Knowledge Transfer Per Level 8.5 URL Generation 8.6 Gamification	3 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5
7	Pre-Survey 6.1 Main Objective 6.2 Survey Details 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization 7.1 Android Elements 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing 7.4.1 General Recommended Behavior 7.5 Conclusion / Summary Approach for Our Anti-Phishing Education App 8.1 App Design 8.2 Game Rules 8.3 Leveling Strategy 8.4 Knowledge Transfer Per Level 8.5 URL Generation 8.6 Gamification	3 4 4 4 4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5
8	Pre-Survey 6.1 Main Objective 6.2 Survey Details 6.3 Evaluation Teaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization 7.1.3 Android Elements 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing 7.4.1 General Recommended Behavior 7.5 Conclusion / Summary Approach for Our Anti-Phishing Education App 8.1 App Design 8.2 Game Rules 8.3 Leveling Strategy 8.4 Knowledge Transfer Per Level 8.5 URL Generation 8.6 Gamification	3 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5

9.3	User Recruitment	ϵ
9.4	Study Design	ϵ
9.5	Results and Discussion	ϵ
9.6	Conclusion	6
10 Con	nclusion and Outlook	6
10.1	1 Conclusion	ϵ
10.2	2 Outlook	ϵ

Zusammenfassung Introduction This chapter introduces the target of this work, which is to design, implement and evaluate an educational app which is supposed to teach unexperienced people to detect phishing attacks. At first we are going to motivate the benefit of our work and how we envision our approach to achieve our goal. Next, we define our specific objectives and point out the major challenges security education poses. Finally, we provide an overview of the following chapters. 1.1 Motivation 1.1.1 Statistics 12 13 1.1.2 Consequences 1.1.3 Technical Solutions 1.1.4 Anti-Phishing Education on the Smartphone 1.2 Goals 20 21 We begin with stating our primary goals of this thesis and describe them in more depth subsequently. The goals of this 22 thesis are to extend, not replace, the technical solutions by 23 1. Increasing the user awareness 24 2. Educating the user 25 Goal description ... 27 1.3 Our Approach 28 29 In the succeeding, we elaborate on how we are going to approach the challenges mentioned before. The reasoning for 30 our approach follows in Section 3.4. 31 32 1.4 Outline 33 This thesis consists of ... main chapters: Their purpose is as follows: 35 Chapter 1 motivates this work... 36 Chapter 2 ... 37 Chapter 3 ... 38 39 Chapter ... finally summarizes this work and provides an outlook on future work. 2 Background 41 Introducing sentences... 2.1 Definition of Phishing 44 45 Our goal is to educate users to detect phishing websites. Since phishing is important in our work, we are going to define 46 our understanding of the term. 47 "Definition of Phishing" 48

The next section dwells on different phishing types.

2.2 Phishing Techniques

- 52 In this section we are going to describe the different phishing techniques that are distinguished in literature. Furthermore
- we state and reason which technique(s) of phishing we focus on in our work.. Phishing techniques include, but are not
- 54 limited to:
- 55 Deceptive Phishing
- 56 Malware Based Phishing (including keyloggers and screenloggers)
- 57 Host File Poisoning
- 58 DNS Based Phishing (Pharming)
- 59 Man-in-the-Middle Phishing
- 60 For our research, we focus on deceptive phishing...

2.3 Phishing Attack Channels

- 63 E-Mail
- 64 SMS
- 65 Instant Messaging
- 66 Online Social Networks
- 67 Fake Website
- 68 VoIP
- 69 Malicious Downloads
- We focus on fake websites. Usually, the links to fake websites are distributed via e-mails, SMS, instant messengers or online social networks, Thus, our approach automatically covers the attack channels e-mail, sms, instant messaging and online social networks.

2.4 Variations of Phishing

- 75 Do we need this subsection?
- 76 Mass Phishing
- 77 Spear Phishing
- 78 Persistent Spear Phishing
- 79 Clone Phishing
- 80 Whaling
- We cover in particular mass phishing. However, the URL checking can be applied in case of any variant, as long as the attack is executed via a fake website.
 - 2.5 Summary Phishing in this Work

3 Related Work

In the following, we present a survey of approaches to anti-phishing education.... We divided the related work we have found in literature into two dimensions: the *communicated content way of communication*

89 90	3.1 Communicated Content
91	General Knowledge Transfer
92	E-Mail Based Knowledge
93	URL Based Knowledge
94 95	3.2 Way of Communication
96	Game Based Learning
97	Quiz Based Learning
98	Comparison Based Learning
99	Emdedded Learning
100 101	3.3 State of the Art
102	Examples here (e.g. Anti-Phishing Phil and Phyllis)
103 104	3.4 Pro and Contra Discussion
105 106	4 System Requirements, Assumptions and Limitations
107	Introductory sentences
108 109	4.1 System Requirements
110	Android OS
111	Version
112	Android Standard Browser (transfer of knowledge to other browsers possible)
113 114	4.2 Assumptions
115	Secure DNS
116	Secure Smartphone
117	No Before-Click URL Analysis
118	Download URLs Possible
119 120	4.3 Limitations of Our Approach
121	Cross-Site Scripting
122	URL Hiding Techniques
123	5 Target Group
123 124 125	Introductory sentences DIVSI
126 127	6 Pre-Survey
128	Introductory sentences

6.1 Main Objective 129 130 6.2 Survey Details 131 132 6.3 Evaluation 133 134 7 Teaching and Learning Content 135 136 In this section we will describe and elaborate on different teaching and learning contents which can potentially be 137 communicated to the user. At the same time we will reason our decision whether to communicate the specific content or 139 7.1 Phishing URLs 140 141 Focus on distinguishing phishing URLs from legitimate ones. 142 7.1.1 Phishing URL Categorization 143 144 Potential phishing URL categories/phishing attcks on URLs 145 Subdomain covered IP Address covered Nonsense Domain covered 148 Trustworthy, But Unrelated Domain covered Similar and Deceptive Domains covered Typo, Typosquatting (Buchstabendreher), Misspelling 150 Homographic Attack covered (the type of homographic visible by user...) Tiny URLs Not covered 152 Cloaked URLs Not covered - because redirect (use of @) Encoding Tricks Not covered - because redirect 154 7.1.2 Problems and Challenges With The Categorization 155 156 7.2 Android Elements 157 158 Invisible Address Bar Find URL Bar, Browser 159 Use of Https Within Websites Browser 160 Analyze Complete URL Via Address Bar Browser 161 Show URL Before Click In E-Mail (not always possible), while surfing (long touch) 162 Copy and Paste URL too much effort, additionally: redirects still possible 163 7.3 Android Browser Security Indicators 164 165 Https Padlock Browser 166 Displayed Webaddress on Https Sites Browser 167 Certificate Verification Touch Padlock to see whole URL.. problems: see document...

7.4 E-Mail Spoofing 170 171 From Field not trustworthy 172 E-Mail Content in hand of attacker 173 Links in E-Mails do not necessarily go where it claims to go (not only in e-mail links). 174 7.4.1 General Recommended Behavior 175 176 Do Not Click 177 Do Not Download Attachment Look at URL **Data Economy** 180 **Date Entry Via Https** 7.5 Conclusion / Summary 182 183 Summarize what to communicate to user here... 184 8 Approach for Our Anti-Phishing Education App 185 186 This chapter presents our final approach for the Anti-Phishing Education App.... 8.1 App Design 1. Awareness Part 190 a) From is not from... 191 b) Linktext unequal actual target URL 2. Education Part 193 a) Information Material b) Exercise to Information Material c) Repeat 2.1 and 2.2 with increasing difficulty 196 8.2 Game Rules 197 198 8.3 Leveling Strategy 199 200 Three approaches... 201 8.4 Knowledge Transfer Per Level 202 203 What is taught in each level ... 8.5 URL Generation 205 206 8.6 Gamification 207 208 User motivation 209 **Show Leaderboard Rate** 210 **Show Leaderboard Total** 211 212

	valuation
The :	goal of this chapter is to evaluate our Anti-Phishing Education App which we described in the previous chapter.
9.1	Hypotheses
9.2	Measurement
9.3	User Recruitment
9.4	Study Design
9.5	Results and Discussion
9.6	Conclusion
10 C	Conclusion and Outlook
This work	chapter provides a short summary of what we achieved in the scope of this thesis and presents an outlook on fu
10.	1 Conclusion
The	objectives of this thesis
10	2 Outlook
This	section deals with a prospect on future work for our Anti-Phishing Education App. In particular, we present ic

that might be beneficial and which we were not able to realize due to time and resource limitations.