# **Anti-Phishing Education App**

**Design, Implementation and Evaluation**Master-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 21. 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 21. Dezember 2013	
(G. Canova)	_

# Inhaltsverzeichnis

1	ntroduction	1
	.1 Motivation	1
	·	1
		1
		1
	·	1
		1
	• •	1
2	Background	1
	e e e e e e e e e e e e e e e e e e e	1
	2.2 Phishing Techniques	
	2.3 Phishing Attack Channels	
	2.4 Variations of Phishing	
	2.5 Scope	2
_		_
3	Related Work	2
		3
		3
	Previous work	J
4	ocus	3
•	l.1 Focus	
	4.2 System Requirements	
	Assumptions	
		3
_		
5	arget Group	3
		3
6	Pre-Survey	3
	Pre-Survey 5.1 Main Objective	<b>3</b> 4 4
	Pre-Survey 5.1 Main Objective	4
	Pre-Survey 5.1 Main Objective	4
	Pre-Survey 5.1 Main Objective	4
6	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching and Learning Content 7.1 Phishing URLs	4 4 4
6	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization	4 4 4
6	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching and Learning Content 7.1 Phishing URLs 7.1.1 Phishing URL Categorization 7.1.2 Problems and Challenges With The Categorization	4 4 4 4 4
6	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching 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	4 4 4 4 4
6	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching 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	4 4 4 4 4 4
6	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching 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 7.2 E-Mail Spoofing	4 4 4 4 4 4 5
6	Pre-Survey 5.1 Main Objective 5.2 Survey Details 6.3 Evaluation  Feaching 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 and Challenges With The Categorization 7.1.3 Android Elements 7.3 Android Browser Security Indicators 7.4 E-Mail Spoofing 7.5 General Recommended Behavior	444 444455
6	Pre-Survey 5.1 Main Objective 5.2 Survey Details 6.3 Evaluation  Feaching 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 7.2 Feaching and Challenges 7.3 General Recommended Behavior	4 4 4 4 4 4 5
7	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching 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 7.1 Android Browser Security Indicators 7.4 E-Mail Spoofing 7.5 General Recommended Behavior 7.6 Conclusion / Summary	44444555
6	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching 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 7.5 General Recommended Behavior 7.6 Conclusion / Summary  Approach for Our Anti-Phishing Education App	444 4444555 <b>5</b>
7	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching 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 7.5 General Recommended Behavior 7.6 Conclusion / Summary  Approach for Our Anti-Phishing Education App 8.1 App Design	44444555
7	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching 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 7.5 General Recommended Behavior 7.6 Conclusion / Summary  Approach for Our Anti-Phishing Education App 8.1 App Design 8.2 Game Rules	44444555 <b>5</b> 5
7	Pre-Survey  5.1 Main Objective  5.2 Survey Details  5.3 Evaluation  Feaching 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  7.5 General Recommended Behavior  7.6 Conclusion / Summary  Approach for Our Anti-Phishing Education App  8.1 App Design  8.2 Game Rules  8.3 Leveling Strategy	<b>4</b> 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5
7	Pre-Survey  5.1 Main Objective .  5.2 Survey Details .  5.3 Evaluation .  Feaching 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 .  7.5 General Recommended Behavior .  7.6 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 .	<b>4</b> 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5
7	Pre-Survey  1.1 Main Objective 1.2 Survey Details 1.3 Evaluation  Peaching and Learning Content  1.1 Phishing URLs 1.1. Phishing URL Categorization 1.2 Problems and Challenges With The Categorization 1.2 Android Elements 1.3 Android Browser Security Indicators 1.4 E-Mail Spoofing 1.5 General Recommended Behavior 1.6 Conclusion / Summary  1.7 Approach for Our Anti-Phishing Education App 1.8 App Design 1.9 Game Rules 1.9 Game Rules 1.0 Leveling Strategy 1.0 Knowledge Transfer Per Level 1.1 URL Generation	<b>4</b> 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5
8	Pre-Survey  1. Main Objective 1. Survey Details 1. Sevaluation  Feaching and Learning Content  1. Phishing URLs 1. Phishing URL Categorization 1. Phishing URL Categorization 1. Phishing URL Categorization 1. Android Elements 1. Android Browser Security Indicators 1. Feach Android Browser Security Indicators 1. Feach Conclusion / Summary 1. General Recommended Behavior 1. Gonclusion / Summary  1. Approach for Our Anti-Phishing Education App 1. App Design 1. Game Rules 1. Leveling Strategy 1. Knowledge Transfer Per Level 1. URL Generation 1. Gamification	<b>4</b> 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5
7	Pre-Survey 5.1 Main Objective 5.2 Survey Details 5.3 Evaluation  Feaching 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 7.5 General Recommended Behavior 7.6 Conclusion / Summary  Approach for Our Anti-Phishing Education App 7.1 App Design 7.2 Game Rules 7.3 Leveling Strategy 7.4 Knowledge Transfer Per Level 7.5 URL Generation 7.6 Gamification 7.7 Captron Control Contr	4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5
8	Pre-Survey 1.1 Main Objective 1.2 Survey Details 1.3 Evaluation  Peaching and Learning Content 1.1 Phishing URLs 1.1.1 Phishing URL Categorization 1.1.2 Problems and Challenges With The Categorization 1.2 Android Elements 1.3 Android Browser Security Indicators 1.4 E-Mail Spoofing 1.5 General Recommended Behavior 1.6 Conclusion / Summary  Approach for Our Anti-Phishing Education App 1.1 App Design 1.2 Game Rules 1.3 Leveling Strategy 1.4 Knowledge Transfer Per Level 1.5 URL Generation 1.6 Gamification 1.7 Hypotheses	<b>4</b> 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5

ç	9.3	Participant Recruitment	$\epsilon$
ç	9.4	Study Design	$\epsilon$
ç	9.5	Results and Analysis	$\epsilon$
ç	9.6	Discussion	$\epsilon$
ç	9.7	Conclusion	$\epsilon$
10 (	ີ ດກ	clusion	6
		Conclusion	
1	0.2	Prindings	$\epsilon$
1	0.3	Recommendations	$\epsilon$
1	0.4	Future Work	$\epsilon$

#### Zusammenfassung

• • •

#### 1 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 of Phishing

#### 1.1.2 Consequences of Phishing

# 1.1.3 Technical Solutions to Counter Phishing

# 1.1.4 Anti-Phishing Education on the Smartphone

#### 1.2 Goals

We begin with stating our primary goals of this thesis and describe them in more depth subsequently. The goals of this thesis are to extend, not replace, the technical solutions by

- 1. Increasing the user awareness
- 2. Educating the user
- 3. ...

Goal description ...

# 1.3 Our Approach

In the succeeding, we elaborate on how we are going to approach the challenges mentioned before. The reasoning for our approach follows in Section ??.

•••

#### 1.4 Outline

This thesis consists of ... main chapters: .... Their purpose is as follows:

Chapter 1 motivates this work...

Chapter 2 ...

Chapter 3 ...

•••

Chapter ... finally summarizes this work and provides an outlook on future work.

# 2 Background

Introducing sentences...

# 2.1 Definition of Phishing

Our goal is to educate users to detect phishing websites. Since phishing is important in our work, we are going to define our understanding of the term.

"Definition of Phishing"

The next section dwells on different phishing types.

# 2.2 Phishing Techniques

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 limited to:

**Deceptive Phishing** 

Malware Based Phishing (including keyloggers and screenloggers)

**Host File Poisoning** 

**DNS Based Phishing** (Pharming)

Man-in-the-Middle Phishing

For our research, we focus on deceptive phishing...

# 2.3 Phishing Attack Channels

E-Mail

SMS

**Instant Messaging** 

**Online Social Networks** 

**Fake Website** 

VolP

**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

Do we need this subsection?

Mass Phishing

**Spear Phishing** 

Persistent Spear Phishing

Clone Phishing

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 Scope

# 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 categories: the *content*, i.e. what the user is taught and the *medium*, i.e. how the user is taught.

3.1 Content Classification
General Knowledge Transfer
E-Mail Based Knowledge
URL Based Knowledge
3.2 Medium Classification
Game Based Learning
Quiz Based Learning
Comparison Based Learning
Emdedded Learning
3.3 Previous Work
Previous work here (e.g. Anti-Phishing Phil and Phyllis)
4 Focus
Introductory sentences
4.1 Focus
Based on the discussion of the previous section we decided to
4.2 System Requirements
Android OS
Version
Android Standard Browser (transfer of knowledge to other browsers possible)
4.3 Assumptions
Secure DNS
Secure Smartphone
No Before-Click URL Analysis
Download URLs Possible
4.4 Limitations of Our Approach
Cross-Site Scripting
URL Hiding Techniques
5 Target Group
Introductory sentences DIVSI
6 Pre-Survey
Introductory sentences

#### 6.1 Main Objective

# 6.2 Survey Details

#### 6.3 Evaluation

# 7 Teaching and Learning Content

In this section we will describe and elaborate on different teaching and learning contents which can potentially be communicated to the user. At the same time we will reason our decision whether to communicate the specific content or not.

#### 7.1 Phishing URLs

Focus on distinguishing phishing URLs from legitimate ones.

# 7.1.1 Phishing URL Categorization

Potential phishing URL categories/phishing attcks on URLs

Subdomain covered

IP Address covered

Nonsense Domain covered

Trustworthy, But Unrelated Domain covered

Similar and Deceptive Domains covered Typo, Typosquatting (Buchstabendreher), Misspelling

Homographic Attack covered (the type of homographic visible by user...)

Tiny URLs Not covered

Cloaked URLs Not covered - because redirect (use of @)

Encoding Tricks Not covered - because redirect

# 7.1.2 Problems and Challenges With The Categorization

# 7.2 Android Elements

Eventuell Titel umbenennen, anders strukturieren...

Invisible Address Bar Find URL Bar, Browser

Use of Https Within Websites Browser

Analyze Complete URL Via Address Bar Browser

Show URL Before Click In E-Mail (not always possible), while surfing (long touch)

Copy and Paste URL too much effort, additionally: redirects still possible

# 7.3 Android Browser Security Indicators

Https Padlock Browser

Displayed Webaddress on Https Sites Browser

**Certificate Verification** 

Touch Padlock to see whole URL.. problems: see document...

# 7.4 E-Mail Spoofing

From Field not trustworthy

E-Mail Content in hand of attacker

Links in E-Mails do not necessarily go where it claims to go (not only in e-mail links).

#### 7.5 General Recommended Behavior

Do Not Click

Do Not Download Attachment

Look at URL

**Data Economy** 

Date Entry Via Https

# 7.6 Conclusion / Summary

Summarize what to communicate to user here...

# 8 Approach for Our Anti-Phishing Education App

This chapter presents our final approach for the Anti-Phishing Education App....

# 8.1 App Design

- 1. Awareness Part
  - a) From is not from...
  - b) Linktext unequal actual target URL
- 2. Education Part
  - a) Information Material
  - b) Exercise to Information Material
  - c) Repeat 2.1 and 2.2 with increasing difficulty

# 8.2 Game Rules

# 8.3 Leveling Strategy

Three approaches...

# 8.4 Knowledge Transfer Per Level

What is taught in each level ...

# 8.5 URL Generation

#### 8.6 Gamification

User motivation

**Show Leaderboard Rate** 

**Show Leaderboard Total** 

•••

9 Evaluation
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 Participant Recruitment
9.4 Study Design
9.5 Results and Analysis
9.6 Discussion
9.7 Conclusion
10 Conclusion
This chapter provides a short summary of what we achieved in the scope of this thesis and presents an outlook on future work.
10.1 Conclusion
The objectives of this thesis
10.2 Findings
10.3 Recommendations
10.4 Future Work
This section deals with a prospect on future work for our Anti-Phishing Education App. In particular, we present ideas that might be beneficial and which we were not able to realize due to time and resource limitations.
References