Design, Implementation and Evaluation of an Anti-Phishing Education App

Design, Implementierung und Evaluation einer Anti-Phishing Education App

Master-Thesis von Clemens Bergmann und Gamze Canova

Februar 2014

TECHNISCHE UNIVERSITÄT DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

Design, Implementation and Evaluation of an Anti-Phishing Education App
Design, Implementierung und Evaluation einer Anti-Phishing Education App

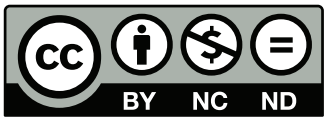
Vorgelegte Master-Thesis von Clemens Bergmann und Gamze Canova

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-37639
URL: http://tuprints.ulb.tu-darmstadt.de/id/eprint/3763

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 February 6, 2014

(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 February 6, 2014

(G. Canova)

Contents

Zusammenfassung

Betrüger entdecken das Internet als einen geeigneten Ort für ihre kriminellen Aktivitäten. Zum Beispiel schicken sie Internetnutzern gefälschte E-Mails, die Links zu wiederum gefälschten Webseiten enthalten. Die Webseiten fordern die Besucher auf, ihre vertraulichen Daten einzugeben. Diese Art von Internetbetrug wird als Phishing bezeichnet. Es existieren verschiedene technische Lösungen, die zum Ziel haben, das Phishing-Problem zu lösen, indem der Benutzer beispielsweise vor dem Zugriff auf eine bekannte Phishing-Webseite gewarnt wird. Diese Ansätze können allerdings keinen rumdum zuverlässigen Schutz garantieren, weil es immer Lösungen geben wird, wie diese Techniken umgangen werden können. Darüber hinaus werden Sicherheitswarnungen und -hinweise solcher Ansätze von den Benutzern nicht immer wahrgenommen oder gar ignoriert. Aus diesen Gründen ist ein komplementärer Ansatz erforderlich. Bisherige Ansätze greifen nicht auf einen entscheidenden Faktor zurück, um der Gefahr zu begegnen - den Benutzer selbst. Die Erhöhung des Bewusstseins für Sicherheit und vor allem die Benutzeraufklärung über die Gefahren des Internets sehen wir als weiteren wichtitgen Schritt in Richtung einer ausgereiften Strategie zur Bekämpfung von Phishing.

Unsere Masterarbeit beschäftigt sich mit der Entwicklung einer Smartphone-App, die das Bewusstsein für Sicherheit erhöht und die Benutzer bezüglich Phishing-Erkennung aufklärt und trainiert. Zur Sensibilisierung des Bewusstseins für Sicherheit, senden sich die Benutzer selbst eine “gefälschte” E-Mail, direkt zu Anfang der App. Der Trainingsteil der App beinhaltet Informationen und Warnungen zu bekannten Techniken der Angreifer und hilft den Benutzern, diese durch Übungen und Wiederholungen zu verinnerlichen. Mit diesen soll der Benutzer die Fähigkeit erlangen, sich in Zukunft vor Phishing-Angriffen zu schützen.

Unsere App ist als Quiz-basiertes Spiel realisiert, die vor allem ihren Fokus auf die Erkennung von Phishing-URLs legt. Um die Wirksamkeit der App zu bewerten, evaluieren wir unsere Anwendung in Form einer Benutzerstudie. Die Studienergebnisse zeigen, dass unsere App den Benutzern hilft bessere Entscheidungen über die Legitimität von URLs zu treffen.

Abstract

Scammers discover the Internet as a convenient place for their criminal activities. For instance, they send Internet users spoofed e-mails which link to fraudulent websites. These websites prompt visitors to enter their confidential data. This kind of Internet fraud is referred to as phishing. There exist multiple technical solutions to approach the problem of phishing which, for example, warn the users against accessing a revealed phishing website. Yet, they all cannot guarantee 100% accuracy since there will always be ways to circumvent these techniques. Moreover, security warnings or indicators of such approaches are not always recognized or even ignored by some end users. For these reasons, a complementary approach is required. Previous approaches do not draw on a crucial factor to combat the threat - the users themselves. Therefore, the increase of security awareness and especially user education about the dangers of the Internet is a further key strategy to combat phishing.

Our master thesis aims at developing a smartphone app, which increases security awareness and educates the user regarding the detection of phishing. To increase security awareness, the users send themselves a “spoofed” e-mail right away when starting the app for the first time. The user education part entails alerts regarding known techniques of attackers and is supposed to assist the users to internalize these with the aid of practice and repetition. By this means, we aspire to help the users achieve the capability of defending themselves against phishing attacks in the future.

In detail, our app is realized as a quiz based game which mainly focuses on the detection of phishing URLs. In order to evaluate the effectiveness of the app a user study is conducted. The study outcomes show that our app helps users make better decisions regarding the legitimacy of URLs.

Acknowledgements

We would like to take this opportunity to thank the people that supported us in developing this thesis directly as well as those whose efforts helped us to focus on this thesis during the last months. First of all, we thank our advisors Prof. Dr. Melanie Volkamer and Arne Renkema-Padmos for their insights and extensive feedback. Furthermore, thanks to Markus Hau for designing some app icons, Peter Mayer for his help and insights with regard to the usage of statistical tests and Stephan Moczygemba for his extensive proof-reading and valuable insights to our thesis. All of them contributed to an enrichment of our work. Finally, we would like to thank our families and friends for their support and confidence. Without their support we would not have been able to focus our attention on this thesis to this extent.

1 Introduction

1.1 Motivation

Nowadays, a world without Internet is unimaginable for most people in developed countries. As an example, 83% of Germany's population has Internet access [1]. The benefits of the Internet are well-known and undeniable. However, the Internet also leads to new kinds of threats. One major issue of today's digitalized world is phishing. Even though many definitions exist depending on the given scenario or technique (cf. section 2.1), phishing can be described as a form of fraud which lures users into disclosing confidential information, usually over fake websites.

According to the website Dr. Dobb's, for example, every day 500 million phishing e-mails are delivered to user inboxes [2]. Commonly, these e-mails are addressed randomly and contain links to those malicious websites. The Anti-Phishing Working Group (APWG) reports that approximately 40,000 unique phishing websites are detected each month [3]. Statistics published by Kaspersky Lab, a well-respected provider for IT security solutions, state that from year 2011-2012 to 2012-2013 the number of attacked users increased by about 87%. While in 2011-2012, 19.9 million users were subject to phishing attempts, in 2012-2013 the numbers climbed up to 37.3 million. Every day about 100,000 Internet users fall victims to phishing attacks, which is twice as much compared to the previous period. An immense increase can also be observed in the number of unique attack sources (i.e. IP addresses), which has tripled from 2012 to 2013 [4]. Finally, RSA and ECM estimate worldwide costs caused by phishing at about $1.5 billion for the year of 2012 [5]. Note that according to Moore et al. [6] phishing statistics might be inherently biased. The problem is, there are several ways to interpret collected data. Hence, every party might assess their data with respect to their interests resulting in diverse statistics. Diversity can also result from setting different foci. Therefore, the reliability of such statistics, including the ones mentioned above, is questionable. Regardless of the reliability and accuracy of the above mentioned statistics it is undeniable that the problem of phishing is prevalent.

Several technical solutions to counter phishing have already been proposed in literature. These include, but are not limited to, e-mail spam filters, URL blacklists, or website takedowns. These systems intend to protect the user from the enormous amount of phishing attempts. Spam filters, for example, sort out phishing e-mails before they even reach the receiver [7, 8, 9]. The major drawbacks of spam filters are that phishers are constantly improving their techniques to circumvent these. Additionally, it is difficult to determine a good thereshold for the aggressiveness of the filters to balance false positives and negatives. Thus, it is possible that phishing e-mails make it through these filters and might harm the user. An alternative approach is the usage of browsers restricting access to or displaying warnings before accessing phishing websites with the aid of so called URL blacklists [10, 11]. The major downside of blacklists is that most of them work reactively. Thus, there is a certain time frame where phishing websites are active without being blacklisted. In this time frame users can access fraudulent websites without being warned or restricted and thus are susceptible to an attack. Even though some dynamic and predictive approaches have been proposed [12, 13, 14], similar to spam filters, there will always be malicious websites which can bypass protective systems (false negatives). Furthermore, the weakest link in the security chain is the user: there exist users who ignore security warnings and thus remain susceptible to phishing and other threats. A field study conducted by Akhawe et al. [15] revealed that 10% of Mozilla Firefox's and 25% of Google Chrome's malware and phishing warnings are clicked through, i.e. ignored. As a matter of fact, such systems are rendered superfluous for users who disregard the warnings. Website takedowns depict another approach to counter phishing. Here, certain parties commonly urge hosting providers to take down revealed malicious websites. Such parties include, for instance, banks, other organizations or specialized takedown companies [16]. The removal of phishing websites is an effective solution, since it implicitly solves the aforementioned problem, where users ignore security warnings: a removed website cannot trick a user into entering sensitive data. Yet, the average life time of a phishing website is 61.69 hours [16], i.e. the site is online and available for 2.5 days during which falling for it remains a threat. Thus, this approach cannot entirely defeat phishing. Obviously, the technical solutions provide protection to a certain degree but cannot assure an overall protection from phishing for two reasons:

1. *Accuracy of Technical Solutions:* First, there will always be false negatives, especially when attackers invent new, more sophisticated deceptions that bypass current prevention systems. Therefore, users should not rely on tech-

nical solutions only. Otherwise there is still the chance that users will fall into the attackers' traps whenever the technical assistance fails.

2. *User Behavior and Knowledge:* Another major issue with technical approaches to counter phishing is user behavior. As indicated above users tend to overlook or deliberately ignore security warnings. If the user behavior does not change such approaches will remain unhelpful for those who do not take them seriously. The problem is that users primarily make use of the Internet for purposes like online shopping, online banking, communicating with relatives and friends etc. Aspects related to security are not of their primary interest. Another factor for overlooking and ignoring these warnings might be the lack of security awareness. Some users might just not be aware of how easy it is for even unexperienced attackers to duplicate a website or send out fake e-mails on behalf of trusted companies or persons. Even if users are aware that there is a certain degree of threat in the Internet, people tend to believe the probability of facing such an attack is very low and that it will not happen to them, until it actually happens to them or to relatives/friends.

The statistics of phishing further support that technical solutions do not seem to suffice. Therefore, we believe that a complementary approach is required to compensate the weaknesses of technical solutions and minimize the threat phishing poses. We regard the raise of user security awareness and the offer of a service for education as a further key step against phishing. Increased security awareness may change user behavior and attitude towards taking the warnings of protective tools more seriously. The user education can help users defend themselves in cases such technical tools fail or also in cases where no tools are available. The opinions on whether user education and increased security awareness will help combat phishing are divided among researchers. There exist security researchers and experts who argue that user education is pointless [17, 18]. Other sources emphasize the need for increased security awareness and education of the users [19, 20]. It also seems that there already exist promising and effective anti-phishing education approaches [21, 22], yet with the need for further improvements which we discuss in section 3. Ultimately, we believe that technical solutions will never suffice to protect the end user entirely. Therefore, there is the need for complementary approaches. The users need to learn that they have to protect themselves and how they can achieve this protection.

1.2 Goals

The major goal of this work is to offer users a service which educates them about phishing so that they are less likely to fall for fraudulent webpages in the future. In detail, the goals we aspire to achieve can be summarized as follows:

1. Increasing the users' security awareness to complement pure technical solutions for countering phishing attempts.
2. Elaborate on both an appealing as well as valuable educational approach which helps the user achieve the capabilities required to identify phishing websites.
3. Evaluate the effectiveness of the approach in a final user study.

The lack of the users' security awareness seems to be a major issue concerning their security related behavior. For this reason we want to raise the users' security awareness hoping that this will increase their attention while it will decrease their vulnerability. Moreover, besides technical solutions and increasing their security awareness, it is important to provide the users with information so that they can learn to protect themselves against phishing attacks in the future. Finally, we want to evaluate the effectiveness of our approach in a user study with respect to whether it actually can help the users protect themselves and how well it is received by them.

1.3 Outline

This thesis consists of eleven main chapters: Introduction, Background, Related Work, Preliminary Considerations Regarding an Anti-Phishing Education App, Target Group, Initial User Survey, App Teaching Content, App Structure and Design, App Development Process, App Evaluation and Conclusion. Their purpose is as follows:

Chapter 1 motivates this work. It describes why phishing is important to address and why technical solutions do not suffice and need to be complemented with user education. Moreover, it states the goals of our work.

Chapter 2 explains background knowledge which is beneficial for the comprehension of our work. It shows that many definitions exist depending on the given scenario or technique and presents our definition of the term "phishing". Furthermore, it points out the consequences of falling for a phishing attack and motivates that our educational service should be implemented as a smartphone app. Finally, it provides an overview of anti-phishing education approaches of previous work.

Chapter 3 gives specific examples of related work. These examples are categorized according to the introduced classes of the previous chapter. Moreover, it states in which way our work is to be distinguished from previous work.

Chapter 4 elaborates on the determination of our scope to educate users about phishing. There, all of our choices are gathered and system requirements are summarized. Furthermore, it explains what assumptions we had to make and states the limitations of our work.

Chapter 5 deals with the target group we want to address with our app. After defining our target audience it explains how the target group can be projected to the German population.

Chapter 6 deals with our initial user survey we had conducted in order to gain some input before elaborating on the app design. After illustrating the main objectives of this survey the chapter presents the results and discusses how the answers influenced our further app elaborations.

Chapter 7 describes and elaborates on different teaching contents which can potentially be communicated to the user. At the same time it reasons our decision whether to communicate the specific content or not.

Chapter 8 presents our final approach for the app design and structure.

Chapter 9 summarizes important steps concerning the development process of our app. This chapter does not provide in-depth insight to our implementation. Instead it gives a brief overview of our approach for the development of a user friendly and understandable app.

Chapter 10 describes our evaluation process. The app was evaluated with the aid of a user study. After introducing our study design, our hypotheses and measurements are stated and explained. Finally, the results of the final user study are analyzed.

Chapter 11 finally summarizes this thesis, gives an insight into our lessons learned and provides an outlook on future work.

2 Background

The objective of this chapter is to provide the required background knowledge for our further design elaborations. We split this chapter into four parts. The first part deals with the term phishing in general which includes common phishing techniques, attack channels, and variations of phishing. This section illustrates the vastness of the term phishing and is intended to narrow it to a definition which reflects the general understanding of it and which we consider in our work. Irrespective of how a phisher obtained sensitive information from his victims, it has consequences for the fooled person as well as for the targeted company. These consequences are briefly illustrated in the second part of this section. As argued in the previous section our intention is to develop a complementary approach to technical solutions which raises security awareness and offers the user an educational service which trains him to detect phishing attempts. We decided to offer this service as a smartphone app which is reasoned in the third part of this section. In the last part we provide a brief overview of anti-phishing education approaches. For better readability and comprehensibility we divided the available approaches into their content, i.e. what specific content is the user told, and the used media, i.e. how is this content communicated to the user. Specific examples of previous work are provided in the next chapter.

2.1 Phishing in General

This section elaborates on the topic of phishing in general. Phishing is a term which is referred to for various scenarios and techniques. Consequently, there are different definitions of phishing found in literature. Therefore, we start with a definition that entails all types of phishing. Subsequently, we introduce different phishing techniques, used attack channels and variations of phishing. Finally, we state our scope with respect to the term of phishing and provide our own definition of it which we consider in this work.

2.1.1 Abstract Definition of Phishing

The goal of this work is to help users distinguish phishing websites from legitimate ones. Since phishing is important within the scope of this work, we define the term first. In fact, phishing is a term that is used by many people in different contexts. Therefore, the following definition is deliberately kept abstract in order to cover all possible scenarios of phishing. At the end of this chapter we will state our definition of phishing which we consider in this work.

"Phishing is the practice of obtaining confidential information from users and describes a form of identitfy theft. Targeted confidential information includes, but is not limited to, user names, passwords, social security numbers, credit card numbers, or account information. " [23]

2.1.2 Phishing Techniques

There are various possibilities how phishers can obtain users' confidential information. In the following we describe phishing techniques that can be distinguished [23, 24]. This is important to know in order to determine what we are able to teach our target group.

Deceptive Phishing: In deceptive phishing social engineering plays a key role. Here, users are deluded into disclosing their confidential data directly to the phisher without being aware of it. A typical scenario is the unsuspecting user receiving an e-mail from an institution he trusts. In fact, this e-mail is malicious and links to a fake website, where the phisher intends to steal the user's data by capturing the fields the user enters trustfully. Once the phisher obtains the user's data, he is able to impersonate the victim's identity and benefit from this.

Malware Based Phishing: As the term already reveals, malware-based phishing embraces some kind of malicious software running on the user's computer. There are several ways of infecting the user's computer with such malware. Social engineering techniques can be used to convince the user to open malicious e-mail attachments or download malevolent files from a website. Another possibility is to exploit security vulnerabilities. Once the malware resides on the target, various technologies can be utilized to get at the users' data. Keyloggers and screenloggers, for example, track users'

data input and send relevant information to a phishing server. Recent research has shown that mobile phone operating systems are as vulnerable to such attacks as desktop systems. Another way is to make use of so-called web trojans, which appear when users intend to log in. While the user thinks he is logging into a website of his trust, the entered information is actually transmitted to the phisher.

The above mentioned phishing techniques are the most common ones which influence the public understanding of the term most. Despite these, there are other possible attacks that could be considered as phishing.

DNS Hijacking: This kind of phishing is also referred to as pharming and includes the manipulation of a system's host file or domain name system (DNS). These kinds of tampering result in returning a fraudulent IP address for URL requests and thus leading the user to a malicious website, even though the URL of a legitimate website had been entered. As a consequence, the unaware user enters his credentials into this fake website and the attacker obtains these which he can misuse. For the user these attacks are almost impossible to detect.

Man-in-the-Middle Attack: In this form of attack the phisher positions himself between the legitimate website and the user. The user's data input is delivered to the phisher, where he stores the information and then forwards it to the legitimate website. Responses are also forwarded back to the user so that the interference of the phisher does not affect the user's interactions. The gained sensitive information can then be sold or misused in any other way. As everything works as usual for the user, it is very difficult for him to detect such an attack.

Content Injection/XSS: Content injection refers to the practice of embedding additional harmful content into legitimate websites. This content can be, for example, malevolent code to log users' sensitive information and deliver the input to the phishing server. Well-known types of content injection include, for example, cross-site scripting (XSS). XSS vulnerabilities result from a web application's usage of content from external sources, such as search terms, auctions or user reviews of a product. This type of data supply can be misused and instead of delivering the expected kind of data malicious scripts can be injected.

Search Engine Poisoning: Other phishing attempts involve search engines. With the aid of common search engine optimization techniques the phisher aspires to rank his phishing website higher than the legitimate website. By doing this he might trick users who use search engines to access websites into visiting his fraudulent page.

2.1.3 Phishing Attack Channels

Several attack channels exist that can be exploited by phishers to reach their victims. This section introduces some possible attack channels [25, 24].

E-Mail: E-Mail spoofing is a common way for a phisher to reach his victims. These e-mails usually imitate renowned institutions, organizations, companies or banks that the recipients trust. They usually contain a text which will deceive the recipient into doing what it says. For this purpose, psychological manipulation techniques are used, including, but not limited to, exerting pressure or issuing threats. Typically a link to a malicious website, whose look and feel is almost identical to the original one, is included. On this website the user is deluded into entering sensitive data which is captured by the phisher. An alternative is the usage of embedded forms in an e-mail where the user fills in the requested data directly instead of being forwarded to a fraudulent website. Finally, sometimes users are even asked to directly send back their confidential data.

SMS: An alternative to acquire confidential user data is making use of cell phone text messages. As with e-mails, the text message may contain a link to a fake website, where the user is induced into divulging sensitive information. The user may also be asked to send back the information directly. Another possibility is being asked to call back a fraudulent or expensive telephone number. This number usually leads to an automated voice response system which is intended to gain the confidential information from the calling user. This form of phishing is also referred to as smishing, derived from the two terms "SMS" and "phishing".

Instant Messaging: Spreading links via instant messages is another way for a phisher to reach his victims. Once the phisher has gained access to a victim's account he can pretend to be him and lure his contacts into disclosing their data as well. The phisher can continue this game repeatedly. Obviously, this kind of deception can be applied in other attack channels, such as e-mails or online social networks, as well.

Online Social Networks: Using online social networks is similar to using instant messaging services. However, online social networks provide additional valuable information to the phisher. With the aid of user profiles and pinboard entries etc. he can make his baits even more credible and trustworthy. For example, with the aid of a social network the phisher might find out that a potential victim likes a specific game. In order to delude this user the phisher might pretend to be the developer of this game, refer to a severe problem with the user's account and ask him to enter his credentials.

Voice Phishing: A further possibility for a phisher is to send out spoofed e-mails asking the victim to call back the telephone number indicated in the e-mail. To deceive the user, the phisher as usual claims to be from a legitimate and trustworthy institution or organization. The number in the e-mail commonly leads to a voice response system by which the user is induced into disclosing confidential information. Alternatively, the phisher may directly call the user. Voice-over-IP (VoIP) further facilitates these kinds of attacks. It makes them easy to execute and inexpensive. Voice phishing is also referred to as vishing.

Physical letters: The phisher might even send out real letters to a number of users. However, we believe that this is unlikely because in contrast to the digital channels, this channel is associated with expenses and more effort.

2.1.4 Variations of Phishing

There exist two major variations of phishing which can be distinguished, mass phishing and spear phishing. As the names reveal, mass phishing involves targeting a large number of users, while spear phishing rather refers to targeting a specific user or group of users. In this section we discusses these two variations.

Mass Phishing: In the case of mass phishing the attacker sends out a tremendous amount of spoofed e-mails to random users. These e-mails usually link to the phisher's fake website where he tricks his victims into disclosing their credentials. In this variation the phisher is not forced or even able to customize the e-mail to the attacked user. He formulates the e-mails such that they might persuade most users and accepts that some users might not fall for it. The principle of mass attacks is very common and effective, since sending e-mails and setting up websites is almost of no cost and effort nowadays. Even if not all phishing e-mails make it through the spam filters or are not opened: sending out a tremendous amount of spoofed e-mails evidently results in a high amount of victims, not in relative, but in absolute numbers. For example, there exist estimations of 156 million phishing e-mails being sent out daily. Only 16 million of these e-mails win the fight against spam filters. The half of these are opened. 800,000 users of these 8 million e-mail recipients actually click on the contained link and still 80,000 users take the bait according to the estimations [26]. As discussed in section 1 the reliability of phishing statistics is questionable. Yet, these number indicate a rough overview of the problem.

Spear Phishing: Unlike mass phishing attacks, spear phishing mainly aims at sensitive information like business secrets, intellectual property or even military secrets. While in mass phishing attacks, spoofed e-mails are sent to millions of random users, spear phishing targets specific individuals resp. groups within organizations to acquire sensitive information. In order to make a deceptive request more credible and personal, information about the targeted individuals and organizations is used. Usually, victims of spear phishing receive an e-mail with a malicious attachment and are induced into downloading it [27]. As sharing documents via e-mail is normal in an organization this does usually not arouse suspicion, if the e-mail is from a known person with a genuine context. This makes spear phishing attacks very hard to detect [27, 28]. When a phisher attacks senior executives or other leaders in positions of influence this is sometimes referred to as whaling [29].

2.1.5 Scope of Phishing in Our Analysis

We showed that phishing is a wide area. Covering it in a whole will go beyond the scope of a masters thesis. Therefore, we have to constrain the scope of this term. In literature phishing is described as the act of gaining sensitive information from unsuspecting users, usually with the aid of fake websites [22, 3, 4]. Here, instead of exploiting system vulnerabilities the users themselves and their trust are exploited. This form of attack is referred to as deceptive phishing. This type of attack is the mostly observed one and influences the public understanding of the term phishing. For this reason, we decided to focus on deceptive phishing.

As aforementioned, phishing websites can be distributed in several ways, including, but not limited to, e-mail, SMS, or online social networks. Additionaly, these services might be accessed via multiple applications (different e-mail applications, dedicated apps, browsers). In order to be independent from the source a link may originate from, we set our focus on the analysis of URLs before entering private data (cf. section 4.1), i.e. on the website itself, such that any attack channel distributing a link to a fake website will be covered by our approach.

Finally, there are two major variations of phishing we introduced. Our main focus is the mass phishing attack, since this is the common one. However, if any spear phishing or whaling attack involves fake websites, this would be covered by our approach as well. Yet, as discussed above spear phishing and whaling attacks are very difficult to detect [27, 28]. Hence, it appears to be reasonable to target this issue separately from mass phishing in further research.

Now that we restricted our understanding of phishing, we provide our definition of the term for the scope of this thesis in the following section.

2.1.6 Our Definition of Phishing

In the following we present our definition of phishing which encompasses our and the genral public understanding of it:

"Phishing is the practice of obtaining confidential information from users and describes a form of identitfy theft. This attack exploits a user's trust rather than system vulnerabilities. More specifically, the user is fooled into believing that he is communicating with a party he trusts and lured into divulging confidential data. This usually happens through phishing websites which look delusively similar to the originals. Targeted confidential information includes, but is not limited to, user names, passwords, social security numbers, credit card numbers, or account information. " [23]

2.2 Consequences of Phishing

Irrespective of in which way the phisher obtained sensitive data, falling for a phishing attack has consequences for the fooled person as well as for the targeted company or organization. In the following some of these consequences are briefly illustrated.

Identity Theft: The main goal of the attacker is to impersonate the attacked party by stealing his credentials. That is to say, a possible consequence of falling for a phishing attack is identity theft [23]. With the obtained information the phisher can, for instance, do online shopping or access the corporate infrastructure on behalf of his victims.

Data Theft: In a private environment the phisher might collect the user's contacts or all kinds of other sensitive information. In case the attacker gains access to corporate systems he might be able to read and copy customer data or other confidential information.

Reputational Damage: When the phisher gets access to a social network account he might be able to deceive "friends" of the victim as well. This might have a negative impact on the victim's reputation. Moreover, if a customer falls for an attack he might blame the targeted company for not protecting him and his data appropriately. Ultimately, this customer might lose confidence in eCommerce operations and the Internet in general.

In another scenario an employee might fall for a phishing trap. If such news reports are published this might undermine the trust of potential and current customers in the attacked company [30, 31].

Financial Loss: An attacker might be able to plunder private or corporate bank accounts which results in financial loss for each victim. Additionally, organizations have to face increased support expenses caused by the problem of phishing [5, 30].

2.3 Anti-Phishing Education on the Smartphone

The goal of our work is to increase users' security awareness and offer them a service with which they can learn to protect themselves against phishing attacks. We decided to implement both an appealing as well as valuable service that incorporates the beforementioned goals as a smartphone app. In the following we reason our decision:

Mobility and Size: The main characteristic of a smartphone is that it is mobile and smaller than the well-known desktop computers. As a consequence, there is less space on the screen. Many browsers, for example, generally hide their address bars due to the lack of space. With the address bar, the URL and other potential security indicators are hidden. The release of iOS7 features a key step towards better transparency for the user. iOS7's Safari browser displays the host instead of the website's title or the URL itself. This might make phishing attacks more difficult to succeed, assumed that users look at and assess this area of the browser. Additionally, in portrait mode the host is displayed even when scrolling down the page, i.e. this relevant information is always visible. An interesting question to ask here is whether, when and how many browsers will follow such an approach. Currently, Android does not support such a functionality. Yet, displaying the host instead of the complete URL or the title only facilitates users to detect phishing. There is still a need for URL parsing comprehension for these purposes.

Distraction Caused by Mobility: Users often use their smartphones while on the move, when walking or during a train or a bus ride, for example. These circumstances imply distractions from the environment. These distractions obviously will influence the user's attentiveness. Hence, smartphone users might be even more vulnerable to phishing attacks than the traditional desktop user. This is also indicated by Boodaei's report [32], which says that mobile users are three times more likely to access phishing websites than desktop users. This might also be affected by the fact that mobile e-mail clients effectively provide no way to check the validity of an incoming e-mail. The potential distraction raises the question whether it has an impact on the user's education and retentiveness. According to the principles of learning (cf. section 8.6.1) it most likely has an impact on the learning performance. Yet, we believe that our exercise and repetition scheme (cf. section 8.6.1) helps users to internalize the learning content despite potential distractions. For further research it would be interesting to test how significantly distractions impact the learning results of our app, though.

High Number of Smartphone Users: In addition, given that the majority of the people use a smartphone on a regular basis in Spain, Germany, Italy, France, and the UK [33], there is a need for the protection of smartphone users.

Overall, educating the user on the smartphone provides two major benefits. First, the user can access the app on the move, even outside of his desktop environment. The app can be used during train or bus rides, or while bridging the time. Moreover, it can be started and continued any time as a sideline. Despite the fact that we mainly aim at users who want to do something about their unknowingness (cf. section 5), we hope that an enjoyable app might reach even more users. Second, we believe it is easier to transfer knowledge of smartphones to desktop computers regarding several aspects. For example, the parsing of a URL can be easily transferred from smartphones to desktop computers, as desktop screens are bigger and a URL is easier to find compared to smartphones. Transferring knowledge from desktop computers to smartphones, on the other hand, raises more complicated issues. The parsing of a URL on a desktop computer, for example, cannot be easily transferred to smartphones. The user needs to know how to access the generally hidden address bar and how to view the complete URL. Icons or security warnings are probably not easy to transfer in any direction since those differ significantly among devices, versions and browsers.

In the following we discuss various anti-phishing education approaches that we divided into the content that is delivered to the users by them and how these specific contents are delivered to the users. After giving a rough overview of these classes we provide in-depth insight to related work in the next chapter.

2.4 Overview of Anti-Phishing Education Approaches

This section provides an overview of anti-phishing education approaches of previous work. For better readability and comprehensibility we divided the approaches into two categories: the *content*, i.e. what the user is taught, and the *medium*, i.e. how the content is taught. These two categories can be further divided into several classes. In the following, we are going to provide an overview of these classes, before we provide specific examples of previous work in the next chapter.

2.4.1 Classes of Delivered Content

The content classification deals with the precise content of learning which is communicated to the user. The objective of this section is to introduce the different classes of learning content that we identified in previous work.

General Knowledge Transfer: Renowned and targeted websites, such as PayPal, eBay or Microsoft provide general and superficial information about phishing [34, 35, 36]. Usually, they deal with questions like what is phishing, how does phishing happen, what are the symptoms of phishing and how to report phishing attempts.

E-Mail Based Knowledge: In this class of content, the users are told about the "anatomy" of phishing e-mails [37, 38]. Particularly, they are informed about what kind of hints in an e-mail give indications for a phishing attempt. Indications can be potentially malicious attachments, impersonal salutation, requesting personal and confidential information as well as exerting pressure and threatening the user with, for example, account closure. The benefit of detecting phishing attempts before even clicking on a link in an e-mail is that the user would not confirm the existence and active usage of his e-mail address to the phisher. More importantly, the user would not unknowingly download malicious software. The problem with the e-mail based approach is that detecting phishing e-mails by looking at their content becomes more and more difficult [39, 40]. Even if today many phishing e-mails exhibit obvious characteristics we expect that phishing e-mails will improve. Therefore, we believe it is likely that these obvious hints will not remain in the future.

URL Based Knowledge: Sending spoofed e-mails with links to fake websites is a common trick of phishers. On the target website the user is lured into disclosing his credentials. Thus, detecting such fake websites is another possibility to protect oneself against phishing. Here, the user is taught to distinguish phishing URLs from legitimate ones [22, 41]. Links to phishing websites are not only distributed by phishing e-mails. Such links can be spread via any communication channel, such as online social networks or SMS. It is even possible to land on a phishing website by just browsing the web. In these situations knowing how to distinguish phishing URLs from valid ones will help whereas knowledge about phishing e-mails in general will not. The problem with this approach is that as soon as the DNS or host file is attacked even for experts it will get difficult to distinguish a phishing website from the legitimate one (cf. DNS Hijacking in section 2.1.2). Also, it is unlikely that the user checks a URL after each click. This is why, the user should develop a strategy when to check a URL (for example, before entering personal data) and when not. Despite its downsides, we believe that URL based knowledge gives the most reliable hint regarding its "origin", i.e. whether a URL in fact belongs to a legitimate website or not. We had a look at the phishing URLs provided by PhishTank [42]. The majority of these URLs were not or only loosely related to the attacked website. If the users would be aware of the importance of the URL and were able to interpret it the phishers would put more effort in forging valid looking URLs. Obviously, there are enough users falling for primitive attacks. Therefore, we think that it is important to inform the users about the significance of URLs and to teach them how to interpret those.

2.4.2 Classes of Applied Media to Deliver Content

The learning medium describes how the learning content is communicated to the user. The objective of this section is to introduce the different classes of learning media that we identified in previous work.

Simple Text: One possible medium to provide information is simple text. It can be delivered in written or spoken form. For example, most people in Germany learn reading in elementary schools with textbooks. Textbooks and lectures are

also commonly used in university education. Providing the user only with text to the topic of phishing makes it possible to communicate almost any kind of content, so that the learning objectives can get as complex as one wishes. Yet, a user's willingness to read a lot of complex text about computer security depends on his motivation. Moreover, some facts can better be transferred with graphics than with text and in modern time there are more interactive alternatives to simple texts that some people might prefer.

Game Based Learning: Game based learning tries to communicate the learning content vividly and playfully through a game. Such a game usually has a "background story" and a "mission" the user has to accomplish [22, 37]. The game design is important and depends on the target group. Previous work in the area of phishing, for example, focused on a fish as starring role in their game (cf. section 3). This might work well for a target group of young age, but will most likely not be appealing to a larger audience. This is also supported by our survey (cf. section 6).

Quiz Based Learning The quiz based approach is a type of a game which relies on a question-answer cycle without using a specific background story [43]. The advantage of a quiz based approach is that it seems to be more appropriate for adults and thus will likely be appealing to a larger audience, which is also supported by our survey (cf. section 6).

Comparison Based Learning: A further way to teach users is to let them compare legitimate websites, for example, URLs, or e-mails, with fake ones. Here, the user has to decide which of the shown examples are the secure ones [44]. We believe that this form of learning would increase the user awareness, as with this approach one could visualize to the user how difficult it can be to distinguish an original from a fake, especially when they appear almost identical. On the contrary, this way of learning does not reflect the reality, which is a major drawback in our point of view. In real life the user does not have the luxury of choosing between two options, he has only one and has to decide whether this option is trustful or not.

Emdedded Learning: The aim of embedded learning is to educate the user on the topic of phishing during his every day life. For this reason, the user is sent simulated phishing e-mails. In case the user falls for this simulated phishing attempt he is notified and gets more information regarding phishing and how to protect himself [45, 46]. This approach benefits from the so called "teachable moment". In the moment the user realizes that he has almost become a victim to a phishing attack, he will be highly motivated to prevent this happening again and thus be highly receptive for input related to this topic. Yet, a study in Germany revealed that the teachable moment renders superfluous in case the users do not realize what is happening [47]. The authors of this study assessed the effectiveness of CMU/APWG's landing page. They found out that people just closed the window immediately after or shortly after landing on the educational page without reading on, because they thought they were on the wrong website and were not aware that they landed on an educational site. Even with an effective landing page, the missing positive feedback is a major flaw of this strategy in our opinion. The user is only notified in case of a mistake and not in case he has successfully discarded the simulated phishing e-mail. A further problem is raised with the implementation of such an approach. Legal issues will arise when sending simulated phishing e-mails which claim to come from a reputable vendor, such as an online shop.

Due to the drawbacks of embedded learning (legal issues) and comparison based approaches (unrealistic) we believe that a mixture of the game and quiz based approach containing relevant informative text is the best way to go. This approach might be more appealing to a larger audience compared to, for example, just offering simple text. Yet, testing whether a quiz and game based approach is in fact more appealing and appropriate remains for future work. At the very least our survey reveals that potential users tend to vote for quiz based approaches in comparison to simple text or a game with a fish as a main character (cf. section 6.3). Regarding the content which will be communicated to the user we decided to focus on detecting phishing URLs for the reasons explored in this section. A major aspect to consider in further research is the knowledge retainment. For this purpose, our approach should be tested in long-term studies and possibly compared to alternative approaches.

3 Related Work

In the previous section we introduced the different classes of learning contents and communication media. Furthermore, we have decided to go for the game/quiz based approach while focusing on URL based knowledge. This section summarizes specific examples of previous work on anti-phishing education. For each class we previously introduced at least one example is illustrated. We especially elaborate on the game and URL based approach as this is the path we take for our approach. Moreover, we state in which way our work is to be distinguished from previous work.

3.1 Game and URL Based Approaches

Several work has been done in this area [48, 41]. However, most approaches are similar to Anti-Phishing Phil [22] the approach we focus on in this section. Anti-Phishing Phil is a game based approach focusing on URL based knowledge. We will extensively discuss this game since the approach we envision resembles Anti-Phishing Phil the most.

Game Design and Rules: The three objectives of this game are the following: (1) learn to detect phishing URLs, (2) where to look for indications in browsers for trustworthy/untrustworthy websites, and (3) learn to use search engines to find legitimate websites. The major focus, however, is set on the detection of phishing URLs. The main character of the game is a little fish, named Phil, who has to grow to a big fish by eating worms. These worms can either be good, i.e. real worms, or bad, i.e. fake worms, with which fishers try to hook the fish off the sea. Good worms of the game are associated with URLs of legitimate websites, while bad worms are associated with the URLs of phishing websites. Phil's task is to feed on legitimate URLs only. He must reject phishing URLs to grow to a big and healthy fish. The game consists of four rounds in total, each round takes two minutes. For correct actions Phil is rewarded with a certain amount of points. If Phil falsely rejects a legitimate URL, he is slightly penalized by having the time left decremented for a couple of seconds. However, if Phil eats a phishing URL he is severely penalized by losing one of three lives. In this way, the authors try to simulate the extent of the real world effects of their behavior, i.e. in reality rejecting a valid URL is not as bad as trusting a phishing URL. Each round the focus of deception techniques is shifted and phishing URLs get more difficult to identify. In the first round the users get introduced to IP address URLs. The second round mainly deals with deceptive subdomain URLs, where the brand name occurs in the subdomain of a URL. In the third round the users are taught about similar and deceptive domains. In the last round finally, the user has to deal with all kinds of deceptions he has dealt with so far.

Feedback: The information material provided to the user is delivered by so called training messages. Anti-Phishing Phil features four kinds of training messages. First, the user gets direct feedback during the game, whether the answer he has given is correct or not and why. Second, the user has the possibility to receive help in case he needs it. In this case, Phil's experienced father will give a tip. Third, at the end of each round a score sheet is displayed, which summarizes the user's answers, whether they were correct or wrong, and why they were correct or wrong. Finally, there are anti-phishing tips in-between the rounds.

Game Evaluation: To evaluate the effectiveness of the game the authors conducted a between-subjects experiment with three training conditions, represented by three groups: (1) existing training material, for example, from eBay or Microsoft, (2) anti-phishing tutorials which were created based on the game, and (3) the game itself. Each group had to decide on ten websites (in total 20) about their authenticity before and after the training step. The results showed that the participants in the game condition performed better than those in the other two conditions.

Positive Sides: All in all, we believe that the approach is a good step towards user education and features many good aspects. In the first place, the game based approach might be an attractive incentive for the user to be educated. Furthermore, the training messages are kept short and simple. Finally, the training messages, especially the ones of help during the game and the score sheet after each round are very valuable. Due to time restrictions we could not consider those kinds of messages.

Downsides and Our Contributions: On the other hand, we believe that this approach has some flaws and thus is not optimal for user education. Even though using a fish as a main character for this game is a funny idea, we do not think that this is an appropriate solution for adults. This is also reflected by the results of our survey (cf. section 6).

Therefore, we do not use a fish as a main character. Our approach will rather be a combination of a game, which includes lives and points, and a quiz, where users are required to answer questions directly, without any background story. As aforementioned, Anti-Phishing Phil's training messages are simple and easy to understand, however, we are afraid that the phrasing is too vague. For example, for IP address URLs Anti-Phishing Phil displays the following alert message to the user: "Don't trust URLs with all numbers in the front". For subdomain attacks the following wording is used "Don't be fooled by the word ebay.com in there, this site belongs to ttps.us". These kinds of messages are susceptible to misinterpretation. Another downside we see, which is ultimately related to the vague formulations, is that the user is not precisely explained how he has to parse the URL in order to make healthy decisions on the authenticity of such. Here again, he is only told that the most important part of the URL is between the "https://" and "/" and that the name of the website is the text right before the "/". In our point of view, this is a imprecise phrasing and there is a lack of emphasizing the importance of the domain, which we do in our solution. Furthermore, the game does not cover some spoofing techniques, which are still relevant in our opinion and thus are covered by us (cf. section 7.4.1). For example, the difference between HTTP and HTTPS is not introduced, as well as the fact that HTTPS websites can also be phishing websites. Furthermore, the game does not explicitly mention that the domain name, the host or even the entire URL can be part of the path to fool the user. Finally, there are different ways of making use of deceptive domains, which were not explicitly covered by Anti-Phishing Phil. For example, homograph attacks (cf. section 7.4.1), typos and scrambled letters should be distinguished in order to exemplify how mean and hard to detect such URL spoofing techniques can be.

3.2 Game/Quiz and E-Mail Based Approaches

Anti-Phishing Phyllis [37] is a game based approach and focuses on teaching the user to detect a variety of phishing traps in e-mails. These include, for example, fake links, attractive offers, urgent requests, or malicious attachments. The main character of this game is a fish named Phyllis. Phyllis has to decide whether potential traps (marked with red bubbles) in a given e-mail are real phishing traps or are harmless by disarming or ignoring them. The playing user gets hints during the game and direct feedback on his actions. Another quiz and e-mail based approach is provided by SonicWALL [38]. The user is shown e-mails consecutively and has to decide whether the displayed e-mail is legitimate or not. The user does not receive direct feedback on his decisions. At the end he receives an overview of the answers he has given and whether they were correct. If the user wants to know why his answer was correct or wrong he has to click on a link to get this information. As aforementioned, teaching users to detect phishing e-mails before even giving them the possibility to land on phishing websites has the advantage that they do not confirm the activeness of their e-mail address, and more importantly, do not have the chance to accidentally download malicious software or be lured into disclosing sensitive information. However, as phishing e-mails become more and more sophisticated, i.e. convincing and credible, and since phishing websites are also reachable via other communication channels, such as SMS, online social networks or just surfing in the Internet, we decided against the e-mail based approach.

3.3 General Knowledge Transfer with Quizzes

There exist online quizzes where the user is asked general questions to the topic of phishing [49, 43]. The design of these online quizzes is based on the association of phishing with fishing. That is to say, a fish is the main character of the quiz, which we do not find appropriate for adult users. Moreover, the number and variety of the questions asked in these quizzes are very restricted. Even if the examples of the quiz based approaches are not optimal for user education, we think that this approach is the most appropriate one for adults as target group. This is also reflected by the results of our survey (cf. section 6).

3.4 Comparison and URL Based Approach

Symantec offers a "race to stay safe" [44], where the user is shown two snapshots of two websites, while one website is a fake and the other one is genuine. Within very short time the user has to compare the snapshots and decide which way is the safe one to go. The focus of this training is set on the URL and address bar. We believe that such an approach is likely to increase the user awareness of how deceptively similar phishing websites can be to the original ones. However,

the approach of comparing two websites is not realistic enough, since the user does not have two websites and does not have the option to choose between them in reality. This is why we did not decide for the comparison based approach. However, adding time pressure to our approach, i.e. simulating a real life situation, is an aspect which might be worth to consider for future work.

3.5 General Knowledge Transfer with Embedded Learning

There are several proposals in literature for embedded learning [45, 46, 50]. One of these is a solution proposed by Jansson et al. where simulated phishing e-mails with links to fake websites or malicious download attachments are sent out to users [45]. The moment a user falls for a trap of these simulated e-mails he receives a notification informing him that he could have fallen for a real phishing attempt. Also, the e-mail includes a link to a website with a training program with general information and tips on how to detect phishing and malicious attachments. After consulting the training program the user is asked to complete a questionnaire in order to verify whether he understood the content of the training program. A very similar approach, the so called PhishGuru [46], is proposed by Kumaraguru. Another possibility is to leave out the step where simulated phishing e-mails are sent to users. Instead actual phishing e-mails are utilized. For example, the APWG and Carnegie University's CyLab Usable Privacy and Security Laboratory (CUPS) work on the project "Phishing Education Landing Page" [51]. The moment a user clicks on a link of a real phishing website which has already been taken down, i.e. the moment the user behaves riskily, he is redirected to the anti-phishing landing page. There he is told that he had almost become a victim of phishing and provided with educational material to this topic. Finally, there is an approach where the intervention does not happen after clicking on a dangerous link, but while surfing [50]. When the user lands on a blacklisted phishing website and is about to disclose his sensitive data, i.e. presses the submit button, the system interferes: the user is warned and given tips on how to detect phishing websites (for example, he is provided with abstract information on the detection of spoofed URLs). As discussed before, all of these solutions benefit from the so called teachable moment (cf. section 2.4.2). A downside of these approaches is that they do only give negative feedback to the user. Consequently, the user is not rewarded when he rejects to click on a phishing link or to submit data on a phishing website, which is an important thing to do in our view. Moreover, the amount of information provided on such an educational website should be reasonable, i.e. the user should not be flooded with information. Otherwise he will not retain or even consult everything. On top of this, it might happen that the user does not understand the situation and just clicks the warning away [47]. In this case there would be no education at all and the approach would render superfluous. To overcome these issues, a reasonable consideration for future work might be to combine embedded learning with another approach, for example, playing an educational game. For example, the website the user is redirected to might contain just the most important information, enough to motivate the user to click on the provided link to an educational game, for instance our app, in case the user is interested in gaining in-depth insight on this topic. In this way, positive feedback can be included and the information can be transferred to the user bit by bit. For now, we do not follow this approach as the step of sending simulated phishing e-mails to users raises legal issues.

3.6 Further Game Based Approaches on Other Computer Security Topics

Besides the proposals for user education on the specific topic of phishing, there exist a variety of other approaches aiming at educating the everyday user on general or other specific topics of computer security. Auction Hero [52], for example, is a simulation game which covers different topics of computer security, amongst other phishing. Its aim is to help users make more secure decisions in the Internet by modeling their regular Internet behavior. Real life is simulated by making security a secondary goal of the game, like it usually is the case with end users. The primary goal of the user, who is a trader, is to build and sell robots, and earn enough money and reputation to ultimately become an "Auction Hero". As in reality, the trader has to pay attention to various security risks, such as weak account passwords, out-dated antivirus software as well as phishing. Phishing, in particular, is dealt with as follows: the playing user receives e-mails within the game. While some of them are legitimate others are not (for example, an e-mail saying that the user has won an auction for an item on which he has never bid). The e-mails include links to websites where the user is asked to enter his in-game login data. An ultimate consequence of disclosing data to a phishing website is that the user will suffer loss of money and reputation. Also, an explanatory warning will be displayed. The user is taught about typical characteristics of phishing,

potential consequences of falling for them, and how to deal with phishing attempts. This approach has the major benefit of simulating actual online behavior and thus provides a realistic context for the user. Additionally, the user does not only learn about phishing, but other security related aspects, such as having strong passwords and keeping antivirus software up-to-date. On the other hand, we want to focus on phishing attacks in detail instead of giving the user an overview of security topics which have to be considered when using the Internet. There exists a variety of other online games and quizzes covering miscellaneous topics of computer security. "Mission Laptop Security", for example, is a quiz based approach where the user's mission is to transport a laptop to a specific destination in a secure manner [53]. During his trip, the user is asked several questions about how to act in different situations. The mission can only be completed if the user gives enough correct answers. Another game covers the topic of network security [54]. Hackers, represented by little red men, are surrounding the user's WLAN area. By clicking on a hacker man a question appears. When the user gives the correct answer, this specific hacker man disappears. When the user gives an incorrect answer all red men come closer to the user's computer in the center of the WLAN area. Others have diverged from computer based games and rather suggested a physical card game primarily intended to increase the users' awareness of needs and challenges related to computer security in general [55]. A further interesting approach is to change sides. That is to say, the user does not play the role of an unknowing user who has to defend himself from attacker's. Instead he is the attacker and his goal is to profit from criminal activities. Data Dealer [56], for instance, provides a game dealing with the topic of data privacy, data abuse and surveillance. The player's, i.e. attacker's, goal is to collect private data of friends, neighbours or any other person, sell the collected data over the black market and set up companies.

4 Preliminary Considerations Regarding an Anti-Phishing Education App

This chapter elaborates on the determination of our scope to educate people about phishing. Here, we gather all of our choices and the corresponding reasoning for our defintion of our scope. These include the various classes of phishing and phishing learning techniques that we mentioned in section 2 as well as new aspects. Subsequently, we summarize the system requirements and what assumptions we had to make. Finally, the limitations of our work are stated.

4.1 Coverage

Deceptive Phishing as Phishing Technique: As outlined in section 2.1, within the scope of this work we focus on deceptive phishing. In particular, we target the detection of phishing websites resp. phishing URLs.

Several Attack Channels: In order to be independent from the source a link may originate from, we set our focus on the analysis of URLs before entering private data, i.e. on the website itself, such that any attack channel distributing a link to a fake website will be covered by our approach (cf. section 2.1).

Mass Phishing as Variation of Phishing: We cover mass phishing, as already stated in section 2.1.4. However, the URL checking can be applied in case of any variant, as long as the attack includes a website which lures the user into typing in his credentials.

URL Based Knowledge as Learning Content: As argued in section 2.4.1 we believe that URL based knowledge gives the most reliable hint regarding its "origin", i.e. whether a URL in fact belongs to a legitimate website or not. This will be the focus of the learning content in our app.

Game and Quiz Based Learning as Communication Medium: As discussed in section 2.4.2, we decided to develop a quiz game to create an incentive for the users and at the same time reach a large audience.

After Click URL Analysis: The analysis of a URL can follow before or after clicking on a link (if a link is involved), i.e. with a URL preview option or directly in the address bar. Analyzing the URL before clicking on it brings several benefits:

1. *No Malicious Download:* If a spoofed URL is detected before clicking on a link the potential download of malicious software can be avoided.
2. *Phisher Obtains No Information:* Recognizing the spoofed URL before visiting the website prevents the phisher from obtaining any information of the user. Such information includes, for example, the activeness and validity of the user's e-mail address.

On the other hand, the before click scenario has severe downsides:

1. *Redirects Not Recognizable:* Many links contain redirects. Such redirects, which can be malicious, are not recognizable before the click.
2. *Unavailability of URL Preview Functionality:* The URL preview functionality is generally available among various browsers. However, the stock e-mail client of Android, for example, does not provide the functionality of previewing the destination URL. Here, the only way to preview the URL is to apply a long press to the link, copy it into the clipboard, paste it somewhere else and then view it. Then, after the analysis the URL has to be sent to the browser. As this involves too much effort, it is likely that no user will follow such a suggestion. Another possibility would be to force e-mail applications to display plain text in general. The problem with this is that this functionality is also highly dependent on the applied e-mail application and covering all possibilities would not feasible.
3. *Deception with URL Preview:* Browsers in general and several other e-mail clients provide options to display the destination URL of a link. Yet, we believe that this should not be communicated to the user for two reasons. First, we are elaborating on a general approach that does not rely on third party e-mail clients besides the default one, which is pre-installed and comes with the device itself. Second, and most importantly, this functionality has the potential to mislead the user. A severe downside of the URL preview is that the end of the preview is cut in case the

URL is too long. Well-crafted URLs might thus look legitimate even though they are not because the most important part of the URL, i.e. the actual domain, was cut out. For example, the subdomains of the URL can be long and well-crafted so that a legitimate looking subdomain is exactly at the end of the preview. This will cause the user to think that the subdomain at the end of the preview is the domain of the URL. Ultimately, the user will trust this URL even he should not.

4. *Users Click Subconsciously:* A study conducted by Karlof et al. [57] revealed that humans tend to develop automatic responses to recurring situations, so called click whirr responses, i.e. repetitively applied actions tend to happen subconsciously. Such click whirr responses include filling out forms or following links in e-mails from trusted senders. Comparing these two, carelessly filling out forms involves more actions than simply clicking on a link. Therefore, we believe it is even more difficult to break the habit of clicking on links compared to re-thinking the action of filling out a form. In conclusion, we do not believe that we can hinder users from clicking on links, but we hope that we can make them re-think their decision of providing their sensitive data to a potentially malicious website.

The after click scenario does not exhibit all these drawbacks which is why we chose to follow this approach. On the other hand, this scenario might suffer from potential malicious downloads and providing information to the phisher (benefits of before click scenario). If a user confirms his e-mail address to the phisher by clicking on a link, further attacks towards this e-mail address are likely to follow. Also, the pure request and displaying of a phishing website might provide additional information to the phisher or even expose the user to attacks. For now, these aspects remain open for further research, as there is no possibility in our target scenario to detect the actual destination of a link before clicking on it.

Considered Browser: The user is only taught browser skills which can be transferred to any other browser. Nevertheless, when the user gets browser screenshots, for example, we made use of the Android standard browser to be sure that most users are familiar with the pictures they are shown.

4.2 System Requirements

Several system requirement have to be met in order to be able to install and play with the final app. In the following we list these requirements.

Android: Currently the mobile phone market is split between two major competitors. Android (81.0%) and iOS (12.9%) [58]. We decided to develop an app for the Android operating system as it has more users. Moreover, we believe we have greater freedom here compared to an iOS app. Android is an open operating system and imposes less requirements and barriers that allow us a quick development and publication of our app [59, 60].

Version: Our initial intention was to develop an Android app for version 4.0 and upward. However, during the app development we encountered that about 24% of all Android users still have Android 2.3.3 to 2.3.7 [61]. For this reason, we decided to modify the code so that these users can also install and use our app.

Samsung Galaxy S3 or S4: It is not necessarily required to install the app on Samsung Galaxy S3 or S4 devices. Yet, we did not have the possibility to test our app (design and functionality) on different devices. The above mentioned devices are those we tested and used for our final user study.

4.3 Assumptions

We have to make some assumptions about the user's system. If one or more of these do not hold the user might not be able to detect that he is a target of an attack, disregarding of his skills. In the following these assumptions are briefly explained.

Secure DNS: We have to assume that DNS is not under the control of the attacker. Our approach is to show the user how to identify phishing attempts by analyzing the URL of the shown page. In fact, this is of no use if the phisher can control the DNS of the user. Therefore, we assume local host files and all used DNS servers as untouched by a potential attacker. We are aware that there exist technical approaches to secure DNS (for example, DNSSEC). However, as these are neither mandatory nor used on the majority of domains we cannot take them into consideration.

Secure Smartphone: We imply that the user's system is in a secure state. This means that the attacker is not able to, for example, exploit browser vulnerabilities, replace the browser or read the user's input.

Secure SSL: For a man-in-the-middle it is possible to intercept sent or received data and to collect the user data directly without notice. Therefore, we warn the user against entering personal data on non-HTTPS pages. For this reason, we have to assume that HTTPS or the cryptography used by SSL is not broken.

No Malware: Sending e-mails with malicious attachments or links to malicious downloads is a form of malware based phishing. In our approach we assume that the attacker does not lure the user into downloading such malicious software, which captures the user's confidential data. We focus on attacks where the user is encouraged to actively provide his sensitive data himself. Yet, we believe that preventing users from being lured into downloading malware is an important aspect. Therefore, in the future our approach should be expanded with regard to this problem.

4.4 Limitations of Our Approach

In addition to the general assumptions pointed out in the previous section, there are limitations of our approach resulting from the chosen target group for our app. As described in section 5, users from our target audience are no computer experts and have neither time nor are they willing to analyze the shown website thoroughly before entering data. Therefore, we do not intend to tell the users about possible attacks that only experienced user might find.

Cross-Site Scripting: Cross-Site Scripting (XSS) is an attack where the attacker enters code, such as a form, into a legitimate webpage. For a later viewer of this page this form seems to be legitimate content of the attacked webpage and he might be deluded into entering personal data in this area. Depending on the attacked webpage this cannot be detected by the user. This is a vulnerability of the attacked webpage and can be prevented by checking user input. Therefore, we think that preventing this attack is in the responsibility of the website owner.

URL Hiding Techniques: As outlined in section 2.3 most address bars in smartphones are generally hidden and reappear only in case the user scrolls up to the top of the website. There is a possible attack where the attacker can prevent the user from scrolling all the way up and instead might display a fake address bar with a valid looking URL. A problem that the attacker has to face is that mobile browsers look very diffently which must be reflected by the fake address bar, a tedious and difficult task. We are aware that such techniques can be exported to a phishing toolkit, sold and used by many phishers. However, attackers do not need such sophisticated attacks yet, because enough users fall for the simple ones these days. We think this is the reason why this kind of attack has not yet been observed in the wild and the reason why we do not consider it as well. Also, this is an issue which can be addressed with the user interface with approaches similar to the iOS7 Safari browser (cf. section 2.3).

We do not teach users regarding these types of phishing. However, we plan to design our app in such a way that these extensions will be easy to realize.

5 Target Group

This chapter deals with the target group we want to address with our app. After defining our target audience we briefly explain how it can be projected to the German population.

5.1 Target Group Definition

In this section we discuss our target audience. The main condition our target users have to meet is that they can learn something from our app. This means users who have too much prior knowledge on the topic of phishing will not benefit from our app. Thus, these users are not addressed by us. In detail our target group can be modeled with the aid of the conditions listed below.

Attackability: The first precondition that all of our users have to meet is that they are possible targets for phishing. Thus, attackability includes a user's disability to detect phishing. Attackability also includes that the users have to use the Internet frequently so that they have a common trust in the web and usually are willing to enter their personal data [62].

Android Users: The second precondition is that the users should use an Android smartphone, otherwise they will not be able to use the app on a regular basis.

Language: The information blocks of our app consist of German texts. Consequently, the target user should be able to read and understand German texts.

Motivation: The distribution plan for this app is to publish it on the Google Play Store and hope that users download and install it. Therefore, the target users must have a general interest in learning to protect themselves. According to a study by Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) [62], there exist Internet users who are self-confident regarding their knowledge and ability to protect themselves in such a way that they are not willing to learn anything else. We will not be able to reach these users.

For our final user study we aspired to recruit participants who hold these preconditions as far as possible. A description on this aspect is given in section 10.5.1.

Subsequently, we discuss how our target group can be projected to the German population.

5.2 Projection to Population

After defining our target group we now want to make sure that we do not exclude too many potential users. In fact, the app can only be useful and successful if a reasonable audience is covered. To prove this we looked at an extensive survey by DIVSI [62]. In this survey the authors first looked at 60 persons in detail and found seven types of Internet users that are depicted in Figure 1. Thereafter, they tried to apply their findings to the German population by interviewing 2,000 representative persons. Figure 2 illustrates the percentage share of the seven Internet types they identified in Germany. We strived to match our preconditions to these Internet types which is described in the following.

Digital Souveräne: This group frequently uses the Internet, and thus is exposed to phishing. Users of this group also usually own a smartphone. However, we have to rule them out because the users of this group are convinced that they already know the problems of the Internet and how to avoid them. Hence, they are unlikely to download our app and will probably reject any training offer.

Effizienzorientierte Performer: This group matches our preconditions. Users of this group frequently use the Internet as well as smartphones. In contrast to the previous group, they are interested in learning something new and see their obtained knowledge as an investment in the future. To reach the users of this group we should show that they can learn something from our app.

Unbekümmerte Hedonisten: This group is also native in the digital world but in contrast to the before mentioned groups, the users of this group are not aware of the problems and frauds therein. In case they are aware of a problem they seek to secure themselves with the aid of automated software instead of dealing with it themselves. Therefore, the users of this group are not likely to be motivated to use our app.

Figure 1: Internet milieus as defined by DIVSI [62]

Postmaterielle Skeptiker: This group is interested in the Internet and uses it frequently. Its users are aware of the problems and frauds raised by the Internet. As they are interested in information on the Internet, especially from official sources, they might download our app. To reach the users of this group we should clearly state that our app originates from a university.

Verantwortungsbedachte Etablierte: This group is regulary online and also uses smartphones. Its users are especially interested in using protection software and actively seek for information on the Internet. They do not believe that they could protect themselves against the dangers of the Internet and actively aspire to change this. Therefore, we believe that this type of Internet users are likely to appreciate our app. To reach the users of this group we should clearly state that this app helps protect themselves.

Ordnungsfordernde Internet-Laien: This group uses the Internet rarely. For this reason, the users of this group are particularly careful when using it and usually do not enter personal data. Besides, they usually do not have smartphones. Thus, it is not likely that they will use our app.

Internetferne Verunsicherte: These users do not make use of the Internet at all. Therefore, they are not exposed to phishing threats.

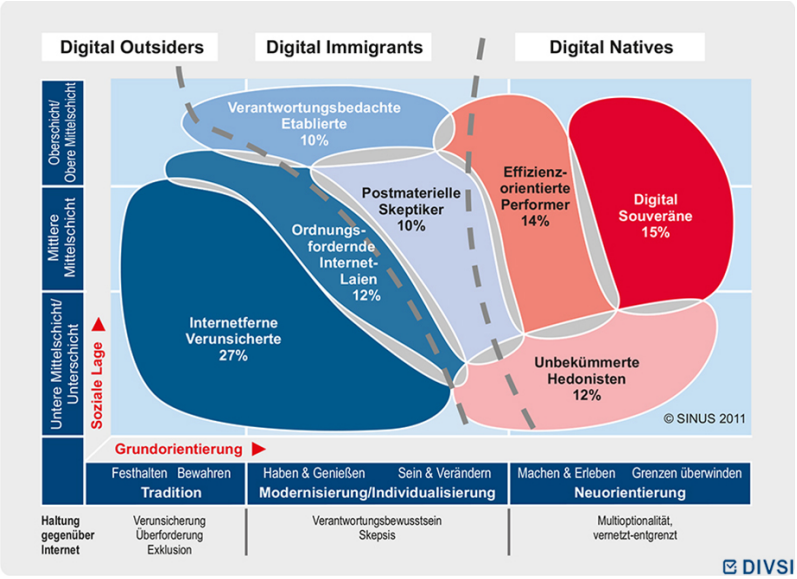


Figure 2: Internet milieus projected to German population [62]

To sum it up, we consider the Internet user types of *Verantwortungsbedachte Etablierte* (10%), *Postmaterielle Skeptiker* (10%), and *Effizienzorientierte Performer* (14%). In total these groups represent 34% of the German population.

6 Initial User Survey

Before elaborating on the app design we ran an initial survey, to gain some input, of which we illustrate the main objectives in this chapter. Furthermore, it provides details regarding the contents of the survey. Finally, this chapter presents the results, evaluates the questionnaire and discusses how the answers influenced our further app elaborations. To the best of our knowledge there do not exist other surveys which resemble ours and additionally were conducted in Germany.

6.1 Main Objectives

Our main objectives of this survey were twofold:

1. *Awareness and Knowledge:* One goal of the survey was to comprehend what exactly Internet users understand under phishing. With a Likert scale we furthermore aspired to figure out how they assess their knowledge on Internet security.

2. *Preferences of Users:* Another purpose of the survey was to get an idea of the users' preferences with regard to an educational app. For example, they were asked whether they found a quiz based approach reasonable for learning purposes.

6.2 Survey Details

This section provides details about our questionnaire, how we distributed it and how we filtered the surveys in order to consider our target group for the results and evaluation. The complete survey form can be consulted in Appendix C.

6.2.1 Questionnaire

In the following we present the structure of our questionnaire and what we intended to achieve with each section of it.

1. *General Information:* In this section the participant is asked to provide information regarding his gender, age, his professional qualification as well as his field of study or work. The main purpose of this section is to exclude participants which do not fit into our target group.

2. *Internet Usage:* Here, the participant is asked how often he uses the Internet, whether he owns a smartphone and which applications he uses on his desktop computer and which ones he uses on his smartphone. This section is intended to give us an overview of the user's Internet usage and helps us exclude participants who do not fit into our target group.

3. *Self-Assessment:* In this part of the survey, the participant has to indicate how much he agrees with the presented statements with the aid of a Likert scale. The statements mainly refer to their self-assessment regarding their knowledge about Internet security. For example, they have to assess, whether they think they have enough knowledge to avoid the dangers of the Internet or whether they think it is easy for them to distinguish legitimate e-mails from fake ones. This section is partially based on Likert scale statements used by DIVSI [62].

4. *Phishing:* Here, the participant gets questions to the topic of phishing. In particular, he is asked which services and which user information are endangered by phishing attacks. This section purposes to find out what the participants know and think about phishing.

5. *Anti-Phishing App:* This section asks the user for his preferences regarding an anti-phishing education app. With the aid of a Likert scale he is requested to assess, for example, whether he likes the idea of a game with a fish, whether he finds text based education appropriate, or whether he would have fun with a question-answer (quiz) game.

6. *Further Survey Progress:* In this part of the survey the user can provide his e-mail address in case he wants to get information about the further progress of the survey or in case he would like to test the app.

6.2.2 Distribution

In total 251 persons participated in our survey. We set up an online survey as well as asked students to fill out our printed survey. In the following we briefly explain our distribution process.

Printed Survey: To reach participants for our printed survey we contacted multiple professors and asked them whether we could have 10 minutes of their lecture time to have their students filled out our printed survey. Moreover, we asked our friends and relatives whether they can ask their friends, colleagues or customers to fill out the questionnaire.

Online Survey: The online survey was mainly distributed digitally. We contacted our friends and asked them to participate in the survey. We also asked to forward the link to their friends to reach a wide range of people.

6.2.3 Select Targeted Participants for Evaluation

Table 1 summarizes what kind of answers we used in order to exclude participants from the survey who do not fit into our target group.

In the succeeding section we present and evaluate the results of the study. With the filtering we had 169 remaining participants matching our target group. These participants were considered for the evaluation.

6.3 Results and Evaluation

The study yielded interesting results which should be considered when designing an anti-phishing education app, either for this as well as for future work. This section outlines the results of the study.

General Information: The gender ratio of our survey participants was more or less balanced. 69 (41%) of the users were male and 96 (57%) of them were female. The remaining 4 (2%) did not indicate any gender. The average age of our participants was 27.59, the youngest participants were 19 years old, the oldest were 63 years old. Most of the survey participators, 82 (49%), obtained a university degree. 42 (25%) of them did not have any professional qualification (yet). 30 (18%) did an apprenticeship and the remaining participants had a master craftsman certificate or did not indicate any professional qualification in the survey.

High Rate of Android Users: The majority of the filtered participants were Android users. In total about 101 (60%) of the study participants used an Android smartphone. The remaining 68 (40%) were iOS users. This result roughly relates to the general market share for these platforms and additionally supports our decision for the implementation of an Android application (cf. section 4.2). Overall, 202 (81%) of the unfiltered participants were smartphone users.

High Internet Usage Frequency: 87 (51%) of the users indicated that they were online several times a day. Another 51 (30%) indicated that they were online even constantly. As a consequence, over 80% of the survey participants are frequently online. This is depicted in Figure 3. Being online is always related with being attackable and vulnerable to dangers of the Internet, such as phishing attacks (cf. Attackability in section 5.1), while the extent of the vulnerability of course also depends on other factors, such as the expertise of the person being online.

Usage Distribution of Internet Applications: Figure 4 and Figure 5 summarize the usage distribution of Internet applications on a desktop computer and on smartphones. Almost all participants, 168 (99%), make use of e-mails on their desktop computer. 150 (89%) of the smartphone owners use their e-mail application on the smartphone, which is still a high percentage. As we previously mentioned in section 2.1.3, e-mail is a common attack channel for phishing attempts. Consequently, all users of e-mail applications, including webmail, are potentially endangered by phishing attacks. The same threat of phishing applies to participants using browsers for surfing. Over 130 (80%) of all considered participants make use of desktop or smartphone browsers. Furthermore, it is conspicuous that banking is far less used on smartphones compared to desktop computers. While about 126 (75%) of the participants make use of online banking on the desktop computer, only 45 (27%) use it on their smartphones, which is still a quarter of the participants. The question to ask here is if these users utilize the browser for online banking or if they use dedicated apps provided by their bank which would

Question	Filtering
Age	We consider all adults ranging from 18 - 65 years.
Gender	We do not exclude any gender.
Professional qualification	The participant does not have to exhibit a specific professional qualification to be considered for the results and evaluation.
Field of study/work	Students, employees or employers in the field of computer science or electrical engineering are ruled out as they do not belong to our target group (cf. Attackability in section 5.1).
Frequency of Internet usage	Participants who have indicated “rarely” as the answer to this question do not belong to our target group and thus are filtered out (cf. Attackability in section 5.1).
Used Internet applications	The listed applications include, for example, browser, e-mail, shopping as well as banking. Any service of the Internet is potentially endangered by phishing. For this reason we do not use this question to sort out participants (cf. Attackability in section 5.1).
Owning a smartphone	With the app we particularly target Android smartphone owners since only those can use our final app on a regular basis (cf. Android Users in section 5.1). Yet, for this particular study we consider it sufficient to own any kind of smartphone. Therefore, participants who do not have a smartphone are ruled out.
Used smartphone applications in the Internet	The listed applications include, for example, browser, e-mail, shopping as well as banking. Any service of the Internet is potentially endangered by phishing. For this reason we do not use this question to exclude participants.
Number of received commercial e-mails per week	We do not sort out out any participants with this question.
Number of received e-mails asking for personal data	We do not sort out any participant with this question.
User reads up on topics related to dangers in the Internet	Participants who have chosen “no” as their answer are filtered out. We specifically target users who are interested in getting safer on the Internet (cf. Motivation in section 5.1). As the participants, who have indicated “no”, do not seem to have any interest in this, they will most likely do not show interest for our app. This is why we regard them as not belonging to our target group and exclude them from the analysis and evaluation.
Section to self-assessment regaring their knowledge about Internet security	We do not sort out participants based on their selection in this section.
Section to questions related to phishing itself	We do not sort out participants based on their selection in this section.
Section to preferences for an anti-phishing education app	We do not sort out participants based on their selection in this section.

Table 1: Filtering rules for the phishing survey

be safer. Whether these users make use of apps or apply their online banking with a regular browser, they might be more likely to react to phishing e-mails on their smartphone, which claim to come from their bank, compared to other users who manage their financial arrangements on a desktop computer and thus are less likely to access a phishing website over their smartphone (cf. section 2.3). To sum it up, all the listed categories of applications are used by the participants, on their smartphones as well as on their desktop computers. For this reason, we decided to use a broad range of URL examples of different website categories for the final app. For future research, one could consider to put the main focus on URLs from specific categories which are mainly targeted by phishing attacks and depend on the usage distribution.

Self-Assessment - Knowledge to avoid dangers of Internet: 31 (18%) of the participants strongly agree that they have enough knowledge to avoid the dangers of the Internet. Further 77 (46%) agree with the statement and only about 22 (13%) disagree or strongly disagree with this statement. As a consequence the majority of the participants are quite confident that they can avoid the security related risks raised by the Internet. The general question to ask in these self-assessing statements is how well they reflect the reality. In this case it is questionable whether 64% of the participants are in fact capable of protecting themselves against the threats of the Internet.

Self-Assessment - Distinguish legitimate from illegitimate e-mails: 149 (87%) of the participants think that they can easily distinguish legitimate e-mails from fake ones (they agree or strongly agree). Only about 13 (8%) of the participants did not agree or strongly disagreed with this statement. This arouses the suspicion that the users are not aware of how easy it is to spoof the “from field” of an e-mail, or to create credible message contents which in fact may persuade the receiver that the e-mail is trustworthy. Therefore, we believe that the user should be made aware of this misconception. For this reason, the part of the app which is supposed to increase a user’s security awareness addresses this issue (cf. section 8.1).

Self-Assessment - Trust in e-mails from known parties: The majority of the participants trust e-mails which come from persons they know. Approximately 33 (20%) strongly agreed and 96 (57%) agreed with this statement. Only about 3 (2%) strongly disagreed and about 9 (5%) of the participants disagreed with this statement. This again shows that most of the participants are not aware that spoofing the “from field” of an e-mail is easy to achieve. These users are likely to react to e-mails which claim to be, for example, from friends. Such e-mails may actually contain links to the download of malware or malicious websites. We address the misconception of believing that e-mails can be trusted, whether they are received from friends or other trusted parties, with our awareness part of the app (cf. section 8.1).

Self-Assessment - Internet security is only related to financial applications: The answers to this statement showed that the majority of the participants are aware that security related issues on the Internet do not solely concern financial applications. 84 (50%) of the users strongly disagreed with this statement and another 41 (24%) disagreed. Only about 17 (10%) of the participators agreed or strongly agreed with this statement and about 24 (14%) indicated “neither nor” as an answer. Even though most users seem to be aware that Internet risks do not only concern financial applications, the ones who are not aware that phishing, for example, can also occur in online social networks, should be enlightened about this. In order to address this issue our initial plan was to display the consequences of falling for a certain phishing website, i.e. phishing URLs. In this way, the user could have learned what his loss could have been, projected to a real-life scenario. This would have contributed to his awareness, in particular that Internet security issues, in our case phishing, are not necessarily related to financial loss only. For time reasons, we were not able to realize this approach. However, it is something that should be considered in future research.

Services Endangered by Phishing: Figure 6 summarizes the results for this question. All in all, we can observe that the participants agree that phishing can actually occur in association to any service. 164 users (97%) agree that especially the e-mail service is endangered by phishing. Also 119 (70%) see the browser, 141 (83%) online banking and 126 (74.56%) social networks as endangered. Still about 68 (40%) consider various media (audio and video) services as well as online games as endangered. These services are in fact not targeted as often as other services on the Internet, however they are potential targets and should be communicated to the user with the aid of the choice of the URLs to decide on, for example. Because of that, we chose to cover URLs that are related to a wide range of website categories.

Data Endangered by Phishing: Figure 7 outlines the results of this question and illustrates that the participants agree that any of the listed kinds of data is potentially endangered by phishing attacks. 153 (91%) of the participants expressed

that login data is endangered by phishing. About 151 (89%) agree that credit card information as well as personal data is endangered, too. Ultimately, 129 (76%) of the participants consider PINs and TANs endangered. Consequently, there does not seem to be a major necessity in enlightening users in this area.

Preferences for an Education App: In this section there are three results which support our decision of the app design. First, most of the users (51%) stated clearly against an app that uses a fish as a main character. Second, most of the users either voted for a quiz based game (52%) or did not care (33%). The minority of the participants voted against a quiz based game (13%). Finally, 41% of the users were neutral regarding text based learning programs. For these reasons, we could confirm our desired approach of a quiz based game, with introductory parts that also contain text (cf. section 8).

In this section we discussed our phishing survey and assessed it pointing out the aspects that are important to consider for the final app elaborations. The subsequent section deals with precise learning contents which might possibly be delivered to the user. It reasons whether a possible learning content is transferred to a user and why or why not.

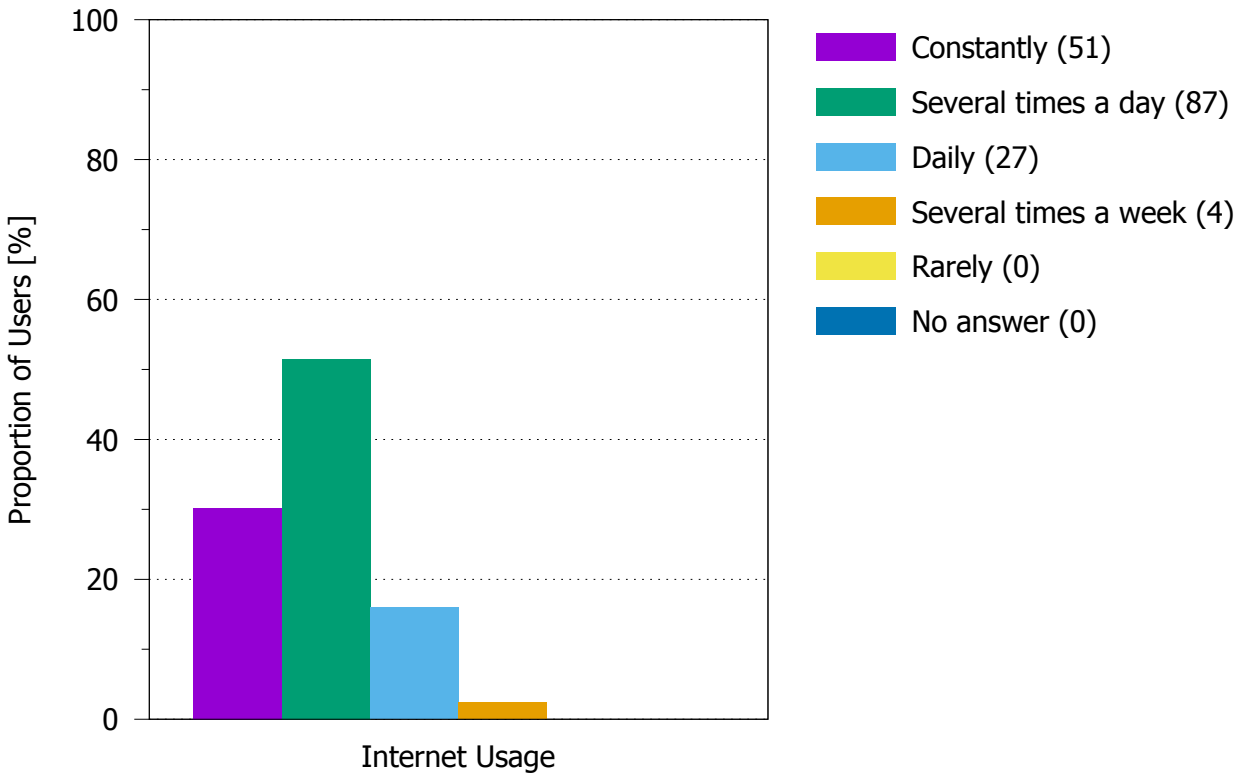


Figure 3: Frequency of Internet usage

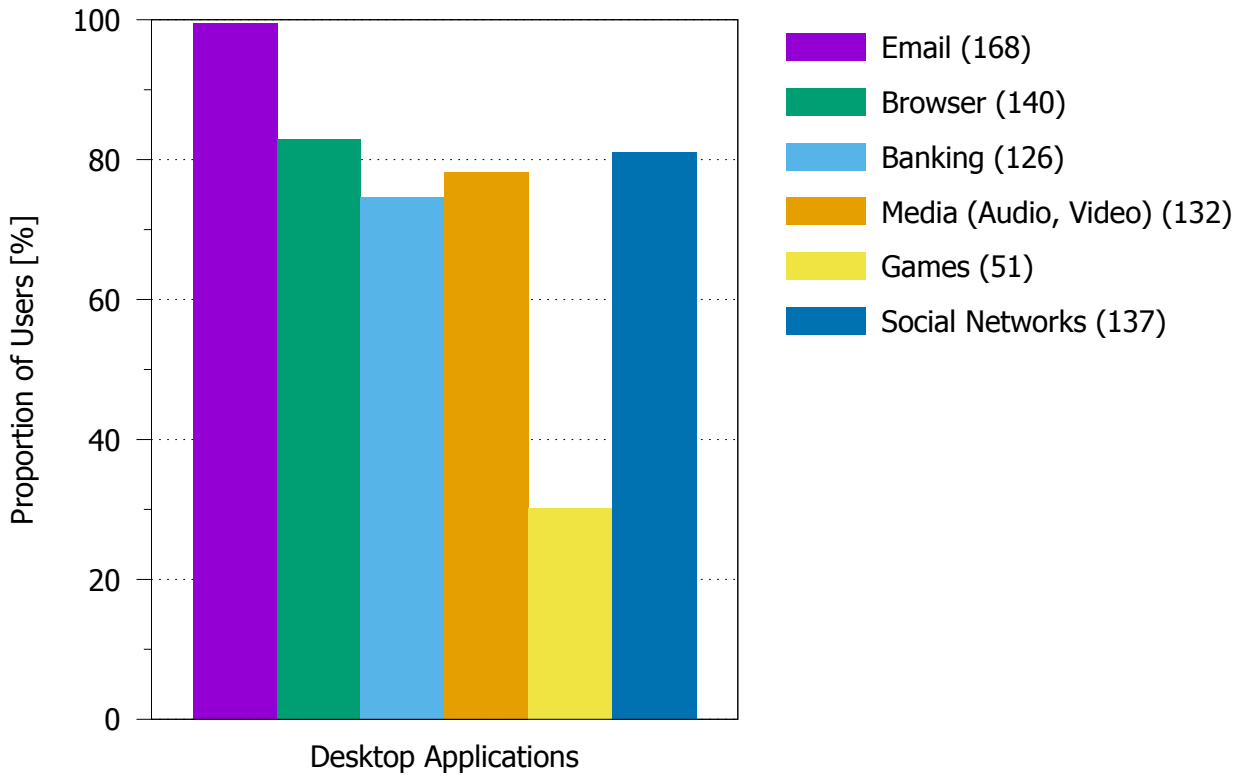


Figure 4: Usage of Internet applications on desktop computers

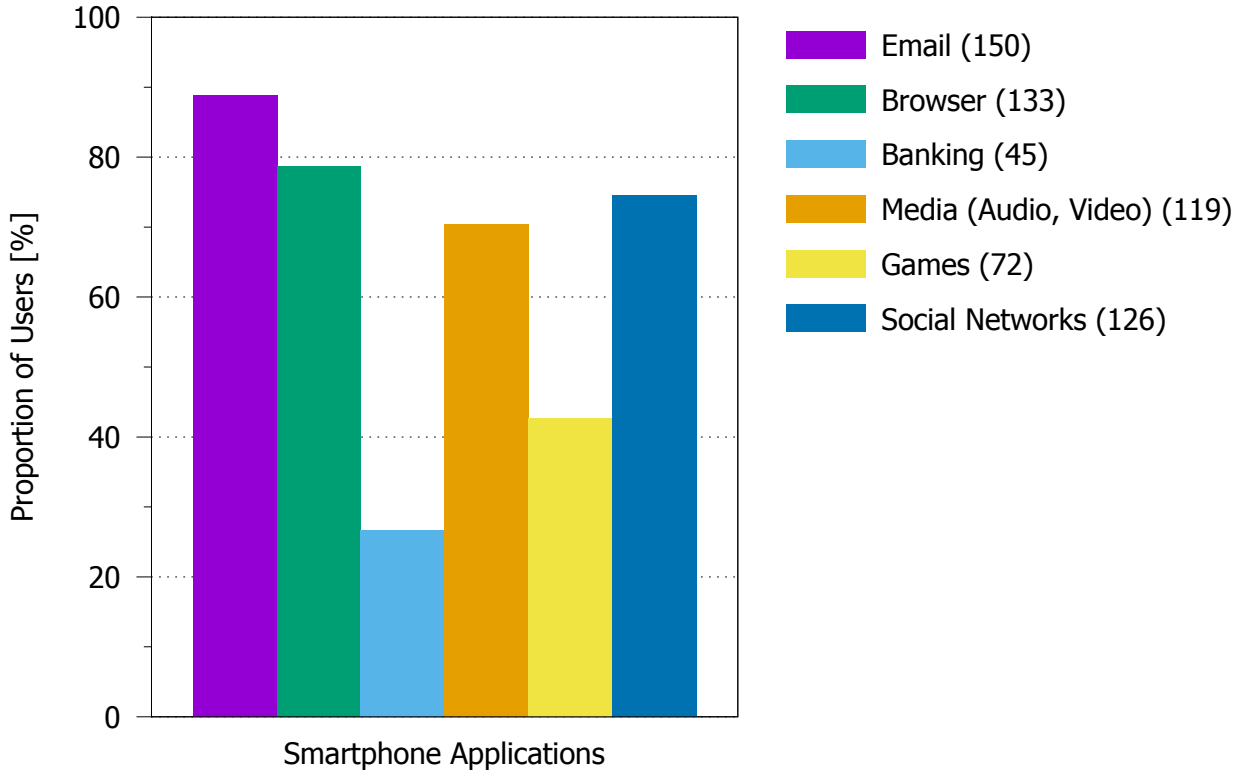


Figure 5: Usage of Internet applications on smartphones

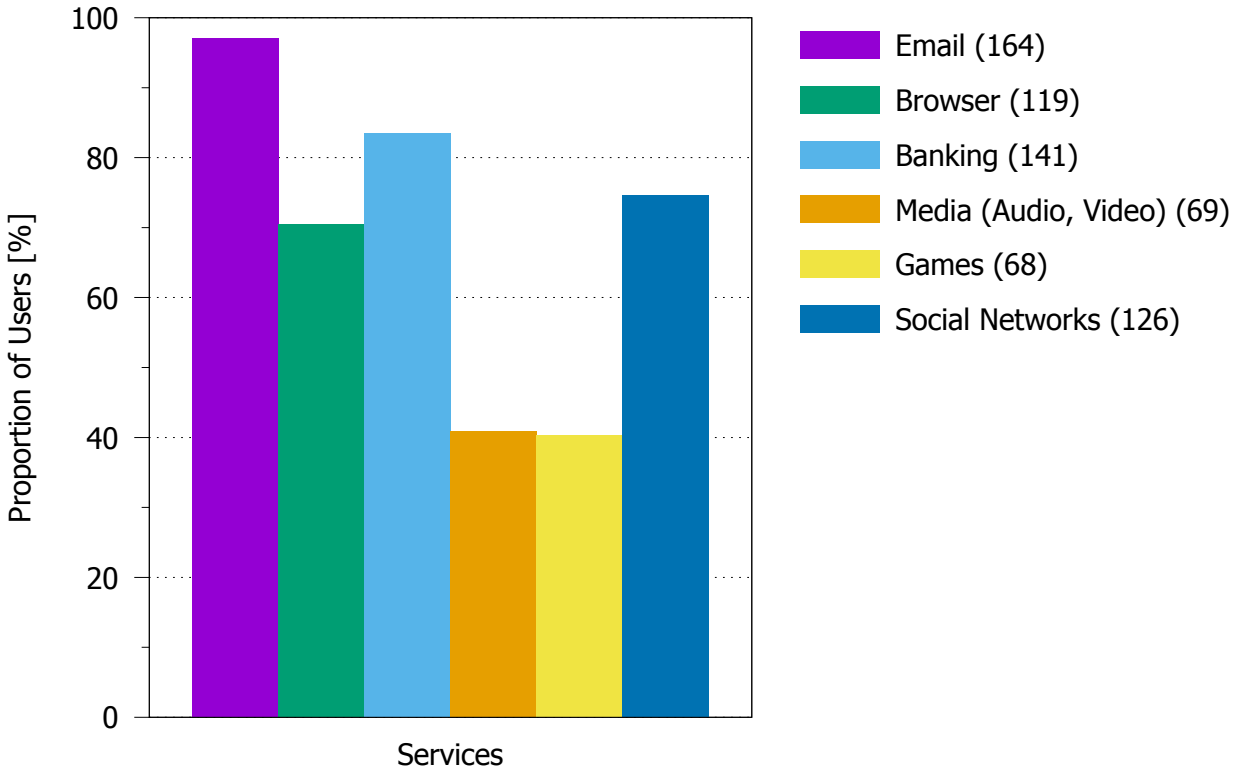


Figure 6: Services endangered by phishing

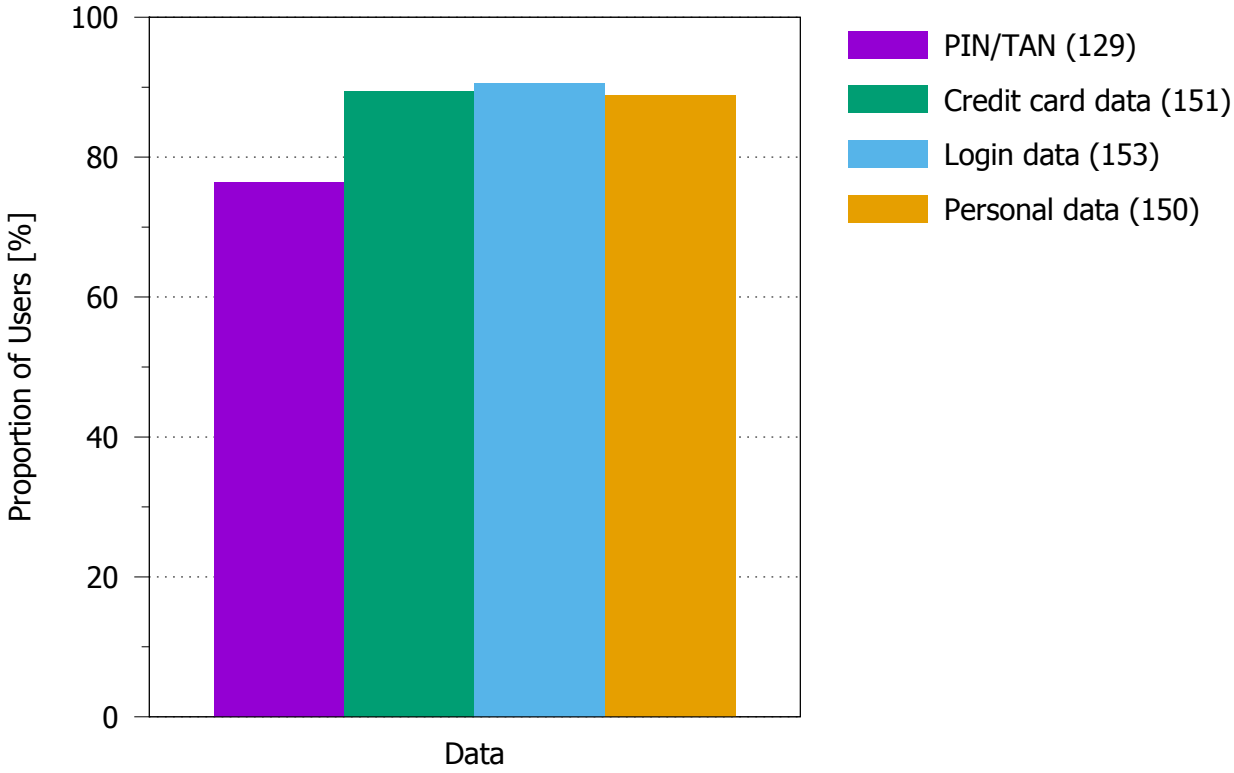


Figure 7: Data endangered by phishing

7 App Teaching Content

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

7.1 E-Mail Spoofing

According to a study by DIVSI [62], 85% of the Internet users utilize e-mails for communication but only 14% have concerns regarding e-mail security. This misconception is also reflected in our phishing survey (cf. section 6). This is a problem because in contrast to public belief e-mail is not secured against fraud. There are three main facts that need to be delivered to the user:

From Field: A major misbelief is that an e-mail's from-field is in some way secured. In reality it must be considered a plaintext field. The problem is that most modern e-mail clients hide this fact away from the user. Therefore, we have to explain to the user that anyone can send e-mails from any from address.

E-Mail Content: We also have to show the user that the content of the e-mail is totally in the control of the sender. Nobody prevents the attacker from sending e-mails that look exactly like the ones sent out by a legitimate sender.

Links in E-Mails: The third aspect that most users are not aware of is that e-mail links or links in general could point to any page. This means that the link does not necessarily lead to the denoted URL.

The above mentioned learning contents are intended to increase the user's security awareness. In section 8.1 we describe how exactly we achieve to communicate these teaching contents to the user.

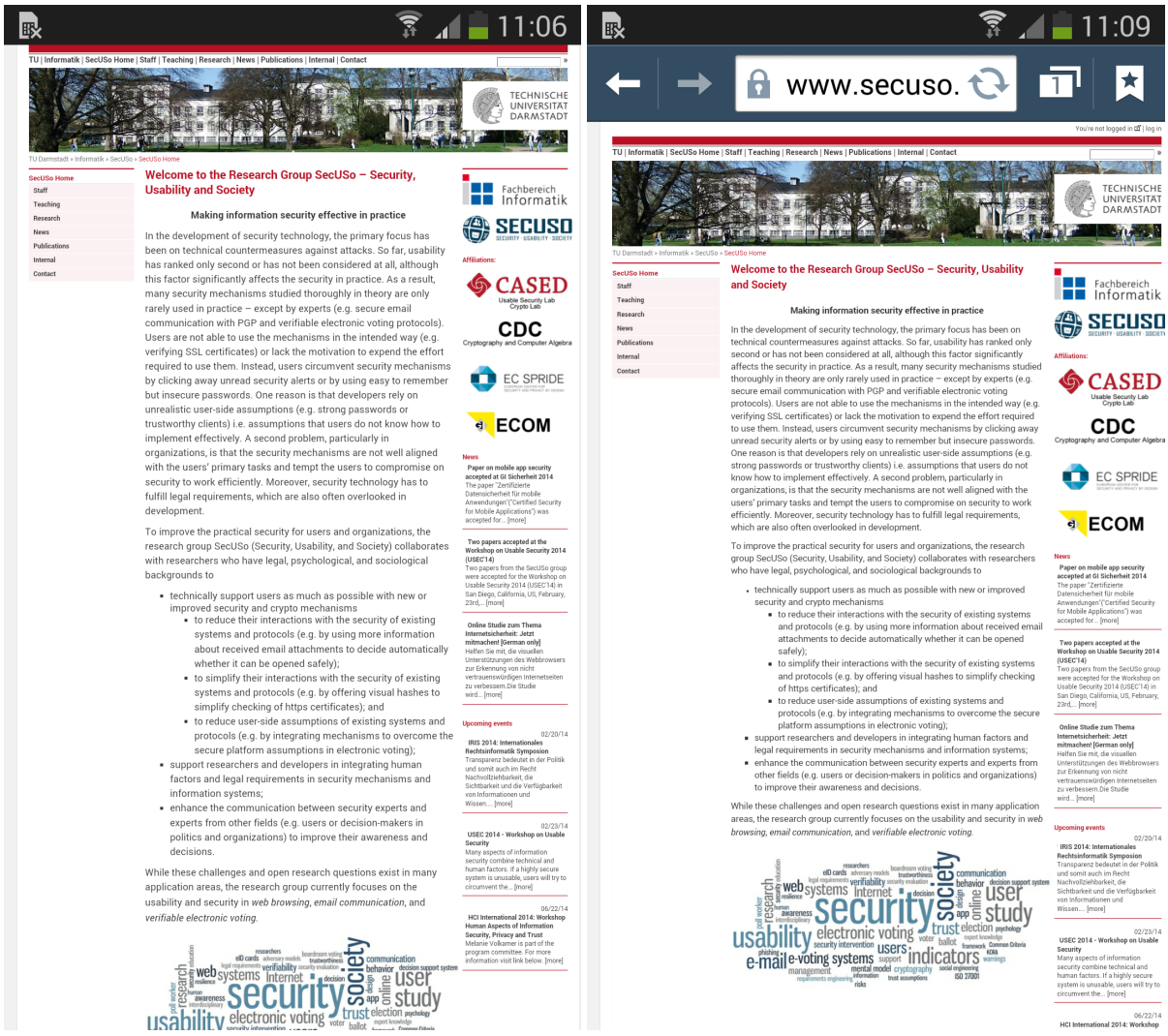
7.2 Smartphone Limitations

As already discussed in section 2.3 smartphones have several limitations, such as the small screen size. This section deals with the detection of phishing on the smartphone and the related limitations. More particularly, we will briefly explain in which ways URLs can be checked with the smartphone and what kind of problems these operations raise. Based on this we decide whether to communicate this kind of URL checking to the user or not.

Invisible Address Bar: As discussed in section 2.3, due to the lack of space most of the smartphone browsers hide the address bar, i.e. the URL, [63] and use this expanded space for the web content (cf. Figure 8(a)). This is an issue which can and should be solved on a technical basis. In fact, some versions of the Android browser already fix this by always displaying the address bar. As long as this is not applied to a majority of active Android systems, this must be communicated to the user because the address bar contains the important information of a website's URL. Most of the users will probably know how they can access the address bar of their browser. However, for those who might not know how to deal with that an introduction is inevitable.

Analyze Complete URL Via Address Bar: Finding the address bar will not suffice for a reasonable URL analysis. Here again, the small screen size makes it is impossible to view the complete URL without any further action (cf. Figure 8(b))). Specifically, it is necessary to first tap the URL address text and then scroll the pointer to the left and right for the URL analysis. Without learning these steps a reliable URL checking is not possible. Therefore, these steps have to be communicated to the user.

Analyze URL After Click: In section 4.1 we extensively discussed the advantages and disadvantages of the URL analysis before as well as after clicking on a link. The reasons why we decided to go for an after click URL analysis can be consulted in that section. Hence, functionalities or workarounds related to showing the destination URL before clicking on a link will not be communicated to the user. Instead we focus on the URL analysis directly in the browser.



(a) Address bar hidden

(b) Address bar visible with padlock

Figure 8: Visibility of the address bar

7.3 Structure of a URL

The URL is a complex construct. In order to correctly analyze a URL and decide whether it is spoofed or not it is necessary to understand its structure. Therefore, the users must achieve the essential capability of parsing a URL appropriately. An attacker uses brands which are familiar to the user in any part of a URL in order to deceive him. Thus, especially the identification of the domain in a given URL is a key aspect which must be covered extensively within the app. We will teach the user about the most important parts of a URL, the protocol (HTTP vs. HTTPS), the host with its domain and the path. We do not distinguish the directory, filename or query parameters of the URL path because this part is rather irrelevant for the detection of phishing. By contracting these elements we can avoid discouraging and overwhelming users with details they do not need.

7.4 Phishing URLs

As aforementioned, we focus on teaching the user how to analyze a given URL and to decide whether it belongs to a legitimate or illegitimate website. In order to distinguish legitimate URLs from phishing URLs it is necessary to analyze existent phishing URLs regarding the way they are spoofed in order to deceive the users. For the analysis of phishing URLs we chose the database of PhishTank [42]. PhishTank is a free community site where people can submit, verify and view phishing data. It provides an API which makes all PhishTank data accessible. Organizations such as Yahoo, Kaspersky Lab and Mcafee use the data submitted by PhishTank. A further reason to choose PhishTank as our phishing URL database was that a contact at Kaspersky Lab himself recommended to make use of it for our URL analysis. For the phishing URL analysis we drew on the URL categories identified by the authors of Anti-Phishing Phil [22] as our baseline. These include IP address URLs, subdomain URLs as well as similar and deceptive domain URLs. Subsequently, we went through the PhishTank URLs and tried to assign them to one of these categories. When no category suited the URL to be assigned, we generated a new category, to which the URL could then be assigned to. In addition, we found various categories mentioned in literature, which we also included to our categories, even if we could not find any explicit example URLs in the PhishTank database. In the following we explain the identified URL categories.

7.4.1 Phishing URL Categorization

URLs are complex and many users do not know how exactly they have to be interpreted. For example, users can be convinced of the authenticity of URL when it contains the brand name anywhere. Phishers exploit this lack of knowledge in different ways. In the following we present the identified categories of spoofing attacks on URLs. All spoofing attacks are covered by the app unless noted otherwise.

Subdomains: Phishers make use of subdomains which are very similar or even identical to the domains of the targeted institutions. For example, they register a domain “xyz.com” and use “paypal” in their subdomain, resulting in a URL such as “http://www.paypal.xyz.com/webapps/”. This makes the users believe that they are on a legitimate website.

IP Addresses: Sometimes phishers do not even bother registering any domain at all. In this case, the host area of the URL contains an IP address.

Nonsense Domains: We frequently encountered URLs which had registered random names or strings as their domain. The domain names ranged from random letters to domain names like “marketstreetchippy.com”. In order to deceive the users some of these URLs contained a well-known brand name in other parts of the URL. Yet, there were a number of examples where this was not the case, i.e. without viewing the content of the website one would have no idea where the URL points to.

Trustworthy, but Unrelated Domains: Some URLs are very well-crafted. When reading them they appear meaningful and trustworthy. This is particularly accomplished by registering domain names which sound reliable, for example, “account-information.com”, “secure-login.de”, or “security-update.com”. If the URL additionally contains the brand name of the targeted institution somewhere in the URL the user can be easily deceived.

Similar and Deceptive Domains: Another possibility to fool users with a spoofed URL is to use URLs which look like the original ones, but have a slight difference. For example, phishers register domains which resemble the targeted domain, but have a typo. To spoof "paypal.com", for instance, the attacker might register "paypel.com". Another approach is to use a modification of the original domain. The modified domain contains the brand name in some form. For example, "facebook-login.com" can be registered in order to fake "facebook.com". Finally, the attacker can scramble letters of the original domain, which can be very hard to detect at first sight.

Homograph Attacks: The homograph attack exploits character resemblance. Here, characters are replaced by other characters which look very similar to the replaced one. For example, an attacker might replace a "w" within a genuine domain with "vv" and register it. An even more advanced way is to replace characters of the genuine domain with characters from other character sets, such as Cyrillic languages, where the characters will look almost identical [64]. The latter case is indistinguishable for the human eye in many cases and is partially a technical issue. Here, browser vendors should be encouraged to indicate when international characters are contained in a URL. For this reason, only cases that are distinguishable by the human eye are covered by the educational app.

Tiny URLs: A tiny URL service is used to convert a long URL into a short one. Due to their shortness tiny URLs are very comfortable to use and easy-to-type. There seemed to be a trend of using tiny URLs for phishing in 2009, in particular in instant messaging services [65]. Tiny URLs usually do not give a hint about the target website and users do not tend to be suspicious about receiving such links from a "friend" what made the use of them for the purpose of phishing quite popular. Tiny URLs redirect the shortened URL to the actual one. As we consider the "analyze URL after click" scenario for the user education, there is no need of the tiny URL to be covered by the app.

Cloaked URLs: Other phishers integrate an "@" into the URL so that domain names become difficult to understand and the actual destination of a link becomes "cloaked" [66]. For example, the URL "http://paypal.com@google.com/" is redirected to "http://google.com". As we consider the "analyze URL after click" scenario for the user education, there is no need of the cloaked URL to be covered by the app.

7.4.2 Problems with URLs

There arise two major problems with the detection of phishing attacks based on the URL.

1. Some legitimate URLs feature characteristics of phishing URLs.
2. We cannot assure that the users know all website vendors of our URLs (whether legitimate or phish).

This section elaborates on these problems and outlines how we approach to handle these issues.

Legitimate, but Fraudulent Looking URLs: We wanted to find out to what extent our determined phishing URL categories from section 7.4.1 apply to authentic websites. For this purpose, we browsed the web and looked at the top 50 banks [67] and top 50 online shops [68] in Germany. While surfing on these websites we recognized that it occasionally happens that a legitimate URL features the characteristic of a phishing URL. This is particularly the case for the category of similar and deceptive domains. There exist sites of vendors which make use of similar domains, instead of never changing the domain and using, for example, subdomains. An example is the website of the Commerzbank. When surfing on Commerzbank's website the domain is "commerzbank.de". Once the user is on the online banking part of the website the domain changes to "commerzbanking.de". The same happens on the PayPal website. The regular website features the domain "paypal.com". However, paypal also has a site, where the domain is "paypal-viewpoints.com". By our definition, "commerzbanking.de" and "paypal-viewpoints.com" contain indications of a phishing website. We decided to address this problem by adding a section of final remarks to the app. In this section we tell the user that there might be legitimate domains which are similar to domains they are familiar with and that these not necessarily are phishes. We still strongly recommend the user to directly contact the vendor before submitting data to such websites. The reason why we do not address this problem in the according level is that we do not want to degrade the user's attention by telling him that similar domains might still be legitimate. We do not consider it an issue that the user is told about this later in the app, since it is better to reject a legitimate URL than trusting a phishing URL.

Unknown Website Vendors: Despite our efforts of mainly making use of URLs from widely known website vendors there is still the possibility that a user does not know all vendors and thus the respective URL. One approach to address this problem is that the user has to indicate which websites he knows with the aid of a long list of check boxes, for example. We decided against this approach for two reasons: First, if a user only knows a few website vendors, the list of available URLs to be drawn from would be quite short. And thus the game experience will degrade significantly. Second, and more importantly, we cannot expect the users to go through a large list of vendors and let them decide whether they know them or not. This kind of configuration would substantially decrease the usability and acceptance of our app. Currently, we have to let the user learn new vendors. By making mistakes and/or giving correct answers to unknown URLs, i.e. domains, the user will likely gain experience and learn whether a given domain is legitimate or not. For future work one might consider to add an "I don't know" button to the options a user has during a challenge in a level of the app. In this case the user could be explained whether it is a phish or not and why it is so. This option should be punished in some way in order to prevent the user from picking only easy URLs for his answers.

7.5 General Recommended Behavior

There are general hints and tips for Internet users which can be helpful to protect oneself against phishing. The user should be informed about these general recommendations at some point. These aspects are explained in the following.

Data Entry Via HTTPS: When the user enters data via HTTP there are basically two problems. First, the user cannot be sure that he actually is communicating with the website it claims to be. Second, even if the user actually communicates with the intended communication partner there still might be an attacker wiretapping the communication. Therefore, data that is sent via plain HTTP is considered lost. This teaching content is covered by our app (cf. section 8.4).

Do Not Download Attachments: Many users download or even open files that they receive via e-mail rather unchecked. This is related to the problem that they trust the from field of the e-mail. It is crucial to tell them that downloading or opening an unknown file might infect their system. As discussed in section 4.3 we assume that users are not tricked into downloading malicious software. This aspect remains open for further research.

Data Economy: The goal of this app is to prevent the users' data from being phished. A further step towards this goal is to teach the user to enter sensitive data as rarely as possible. The idea behind this is that websites, including but not limited to, phishing websites, might exploit user data. For now we put our focus on the detection of phishing URLs. The aspect of re-thinking what data to provide to what kind of service remains an issue to be targeted in future work.

7.6 Browser Security Indicators

As a matter of fact, there is a major lack of mobile browser security indicators [63, 32]. Yet, there exist some, for example, the padlock for the usage of HTTPS. Such signals have the potential to provide relevant information to the user which we would have liked to inform them about. However, besides the lack of such hints there is also the problem of inconsistencies among the mobile as well as desktop browsers. Ultimately, our decision was not to tell anything about these security indicators, as the inconsistencies are too significant even among the standard browser, depending on the device and Android version it is installed on.

HTTPS Padlock All Android standard browsers on various devices we examined have a padlock in the address bar on SSL secured pages (cf. Figure 8(b)). Also, one should consider that there are illegitimate as well as legitimate websites where a padlock is part of the web content. Therefore, it is important to teach the users to look for the padlock in the browser, not in the content, to verify that the site they visit is SSL secured, when they enter confidential data. However, some browsers additionally make use of so called favicons, i.e. small website icons. The danger of using such a favicon is that a phisher could use the image of a padlock in order to deceive the user [32]. Moreover, the padlock with/without favicon combinations appear in different ways. While a part of the stock browsers installed on various devices and Android versions we examined only feature a padlock in case of HTTPS websites and no favicon at all, others always display

favicons. In the latter case, if HTTPS is used the padlock is either positioned right next to the favicon or overlaps it. Due to the variety of possible combinations as well as the deception potential in combination with favicons we decided not to tell the user about the padlock.

Touch Padlock Touching the padlock of an SSL secured website on some browsers leads to an alert dialog with information about the website. One part of this information is the complete URL of the website the user is currently on. In this case, it would become possible to view and analyze the complete URL without tapping the address bar and scrolling to the left and right. For *some* browsers which additionally display favicons, the above described feature is always applicable. That means, the alert dialog with the complete URL can also be consulted on websites which do not use HTTPS. Yet, there are also browsers where neither clicking on a padlock nor on a favicon is possible. Hence, we will stick to our approach, where the user is explained how to analyze the URL directly in the address bar.

Certificate Verification Tapping on the padlock icon in some browsers results in an alert dialog where the user can select to view the certificate details ("show certificate"). As already stated, the padlock feature is not consistent over the various devices and browser versions. Hence, in these cases a validation of the certificate is not possible as well. Therefore, this is an aspect which is not covered by our app.

7.7 Summary

This section briefly lists the above described learning contents which will be addressed by our app. In the following section we precisely explain how the learning contents are reflected in our app and provide further insights to our app design.

1. E-mail spoofing
    a) Do not trust the sender
    b) Do not trust the content
    c) Target URL of a link is not necessarily the displayed one
2. Invisible address bar
    a) Access address bar
    b) View complete URL
3. Structure of a URL
4. Phishing URL categories
    a) Subdomain attack
    b) IP address attack
    c) Nonsense domain
    d) Trustworthy sounding, but unrelated domain
    e) Similar and deceptive domain
    f) Homograph attack
5. General recommended behavior
    a) Data entry via HTTPS only

8 App Structure and Design

This chapter presents our final approach for the app. In the following sections we elaborate on the app design. In detail, we describe how we aspired to achieve our primary goals of increasing the security awareness and providing a service to educate the user on the topic of phishing with the aid of an app. Afterwards, we describe what kind of common gaming elements are included in our app and give a rough overview to the course of the game. Subsequently, we explain the specific teaching goals per level and how we decided to set the thresholds for unlocking the next level. Finally, we provide a summary of basic learning principles and game techniques and to what extent these are reflected in our app.

8.1 App Design

We decided to divide our education app into two main parts. The first part is supposed to increase the security awareness of the users. We also refer to it as "awareness part". The second part of the app then covers the actual educational blocks, also referred to as "educational part". The following listing summarizes the functions of our twofold app structure and Figure 9 graphically visualizes it.

1. *Awareness Part:* The first part of the education app is intended to increase the user awareness regarding how easy it is to spoof e-mails and mislead users with such fake messages. This part is supposed to motivate the user to do something to counter the danger of the Internet and phishing, in particular. It is covered directly after starting the app for the first time and a brief introduction to phishing is provided.

    a) *Receive Fake E-Mail:* We want to illustrate to the user how easy it is to spoof the "from field" as well as the content of an e-mail. For this purpose, the user is displayed a form that allows him to enter a sender (an arbitrary e-mail address), a target e-mail address (user's e-mail address) as well as a text of his choice. Upon submitting the form the user will receive an e-mail from the e-mail address he had indicated as sender. The body of the e-mail contains a common introduction and the user's text of choice. We believe that the user will be surprised about how easy even he himself could send a fake e-mail. Hence, the user learns that he cannot fully trust the "from field" and the content of the e-mails he is receiving. The template for this e-mail can be found in Appendix A.

    b) *Link Text Unequal Target URL:* The awareness part of the app is also supposed to show the user that he cannot trust the texts of a link he is clicking on. To illustrate this, the user is asked to click on a link with the text "https://www.google.de/". Clicking on this link, the user will expect to land on the Google website, what will not happen. In fact, the user is linked back to our app, where he is told that link texts are not trustful as well.

    c) *Fake Website:* Finally, the user is told that creating a copy of a website is also very easy. He is told that a reliable way to decide whether a website is a fake or not is to analyze the URL of the website he is visiting. Ultimately, he is told that this will be the focus of the following exercises.

2. *Educational Part:* The second part of the app covers the actual educational part. Here, the user is learning about various spoofing techniques of the attacker. The second part of the app is divided into levels of increasing difficulty.

    a) *Introductory Block:* The users are first introduced to the lessons to be learned for the current level. These lessons are generally delivered with simple text. Sometimes screenshots or graphics are included. The learning contents of each level are described in section 8.4.

    b) *Exercise* After every introductory block of each level, a corresponding exercise section follows (cf. section 8.4).

    c) *Increasing Difficulty:* There is an increase of difficulty for each succeeding level. That is to say, in each level the tasks become more difficult to accomplish (cf. section 8.4).

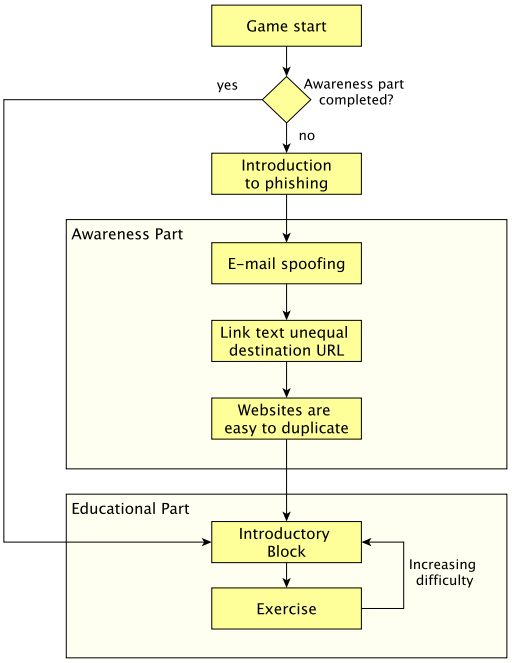


Figure 9: App starting with the awareness and continuing with the educational part

8.2 Gamification

There exist several game elements which are widely used in most modern games. These game elements are reflected in our app as follows:

Lives: An inherent property of a game is the possibility of losing it. If a player is not able to lose a game he will get no positive feedback on having won it. At the same time, one does not want the player to lose the game directly as the result of one minor mistake. Therefore, most games have some kind of "you have N tries"-element, which is commonly referred to as "lives". We included such a mechanism in our app. The details are layed out in section 8.3.

Levels: Most games have some kind of level system. This serves multiple purposes. First, it is important for the player to get a feeling for the progress he makes. Second, it provides fixed points in the game from where he can restart or pause and continue later on. The details of the leveling strategy can be found in section 8.5

Achievements: There exists a type of player who is willing to invest a lot of time in a specific level in order to finish it perfectly or to find every hidden secret in it. To address this type of player modern games offer so called "achievements". Achievements are special elements of a game that a player can unlock if he, for example, finds a special object or if he plays a given level exceptionally well. We implemented achievements for logging in with google+, completing each introductory level and finding 5, 10, 25, 50, 100 and 500 phishing URLs.

Leaderboards: Finally, games often have a leaderboard. A leaderboard is an area where a player can compare his progress in the game with the one of other players. For some people such a leaderboard might have an impact on their motivation and engagement resulting in striving for a better performance. We introduced two leaderboards:

1. *Total Points:* We have a leaderboard that shows how many points the player gained while playing a level. The details of how the points are calculated are described in section 8.5.
2. *Detected Phishing URLs:* We also introduced a leaderboard which displays the user who has detected the most phishing URLs in the app.

8.3 Course of the Game

The educational part, which follows the awareness part, is divided into several levels. This section discusses the course of the game in the educational part. In each level the user is provided with a specific introductory block. After this lecture part is consulted by the user, he has to finish the corresponding exercise.

The first and second information blocks (introduction part 2 and level 1) as well as their corresponding exercises differ from the ones of the other levels. Here, the users obtain basic knowledge in order to balance out inequalities concerning the varying previous knowledge of the players, before the actual game begins.

Obtaining Basic Knowledge: The first information block and task of the user (introduction part 2) deals with accessing the address bar of a webbrowser and viewing its URL completely (cf. section 8.4). After successful completion the user is linked back to the app and level 1 begins. From this level on, the user has three lives upon the start of each level (cf. Figure 10). In level 1 he has to identify the domain of valid URLs (cf. section 8.4). In this level wrong answers result in both, losing points and losing a life. Generally, the user can never get less than 0 points in order to keep him motivated. When the user has no more lives left he has to restart the current level. With every correct answer the user gains points.

The Actual Game: In level 2 we start introducing URL spoofing techniques. All exercises which are followed by the introductory blocks are structured as follows from this point: the user is presented a URL. The user has to scroll the URL to the very left in order to analyze it completely. The scrolling is supposed to simulate the behavior of a browser. The user has to decide whether the presented URL is a phish or a valid URL, by either clicking on the cross or the check mark respectively. The user interface of this challenge part is depicted in Figure 10. Similar to level 1, the user can lose and win points, lose lives and might have to restart a level. Figure 12 illustrates the game flow and consequences of wrong and correct answers from level 2-8. If the user has correctly identified a phishing URL, he has to mark the domain to prove that he has understood the concept. An example view of this proof part is depicted in Figure 11. In all other cases the user is directly shown the result of his answer. We decided that rejecting valid URLs is not as severe as accepting phishing URLs. For this reason the penalty for accepting a phishing URL is stricter (loss of points and a life) than the one for rejecting a valid URL (loss of points). In summary, the user generally loses points for wrong answers, but he does not lose a life for every wrong answer. All in all, the user loses points and a life in the following cases: the user has falsely accepted a phishing URL or the user has correctly rejected a phishing URL, but could not mark the domain correctly. In all other cases of wrong answers the user cannot lose lives, but only points. For correct answers the user is rewarded with earning points and eventually finishing the current level.

8.4 Teaching Goals per Level

This section summarizes the learning objectives of each level. Note that we generally do not use technical terms like URL, domain, subdomain, protocol, or the like. That way, we avoid overwhelming users who might not be able to cope with these technical terms. Figure 14 provides an overview of the level flow in general.

Introduction Part 1: This part is the awareness part described in section 8.1. Here, the user learns how easy e-mail spoofing is. Additionally, the user is informed about the simplicity of setting up fake websites and that he should not trust the texts of the links he is clicking on.

Introduction Part 2: In this part the user is explained how he can access the URL of a web browser and how exactly he has to look at the complete URL. In particular, the user is told that he has to scroll up the whole website to make the generally hidden address bar re-appear. Then he has to tap the text field of the address bar and scroll to the start of the URL. These descriptions are supported with screenshots. For the exercise the user is forwarded to a website. There he has to apply all important steps he just learned in the introductory block and has to provide us the information we request about the URL in the address bar. This will show that he has in fact viewed the complete URL. After successful completion of the tasks, the user is linked back to the app. At the end of the exercise the user is told that he always should analyze the URL like this, because all other displayed URLs or links might be a fake, too.

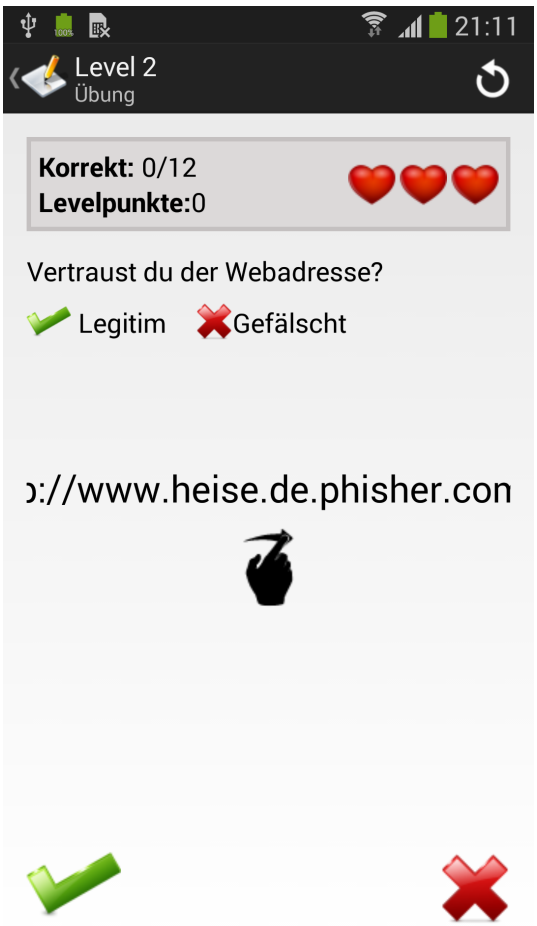


Figure 10: Example challenge view where the user has to decide whether the URL is a phish or not by clicking on the cross or check mark respectively. The user has 3 lives and has to scroll the URL in order to analyze it.

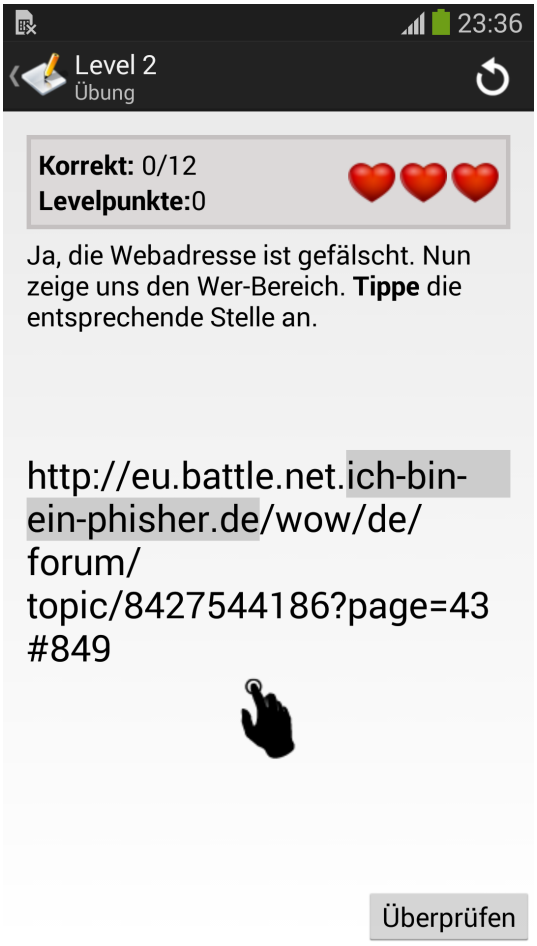


Figure 11: Example view where the user has to mark the domain after correctly identifying a phishing URL

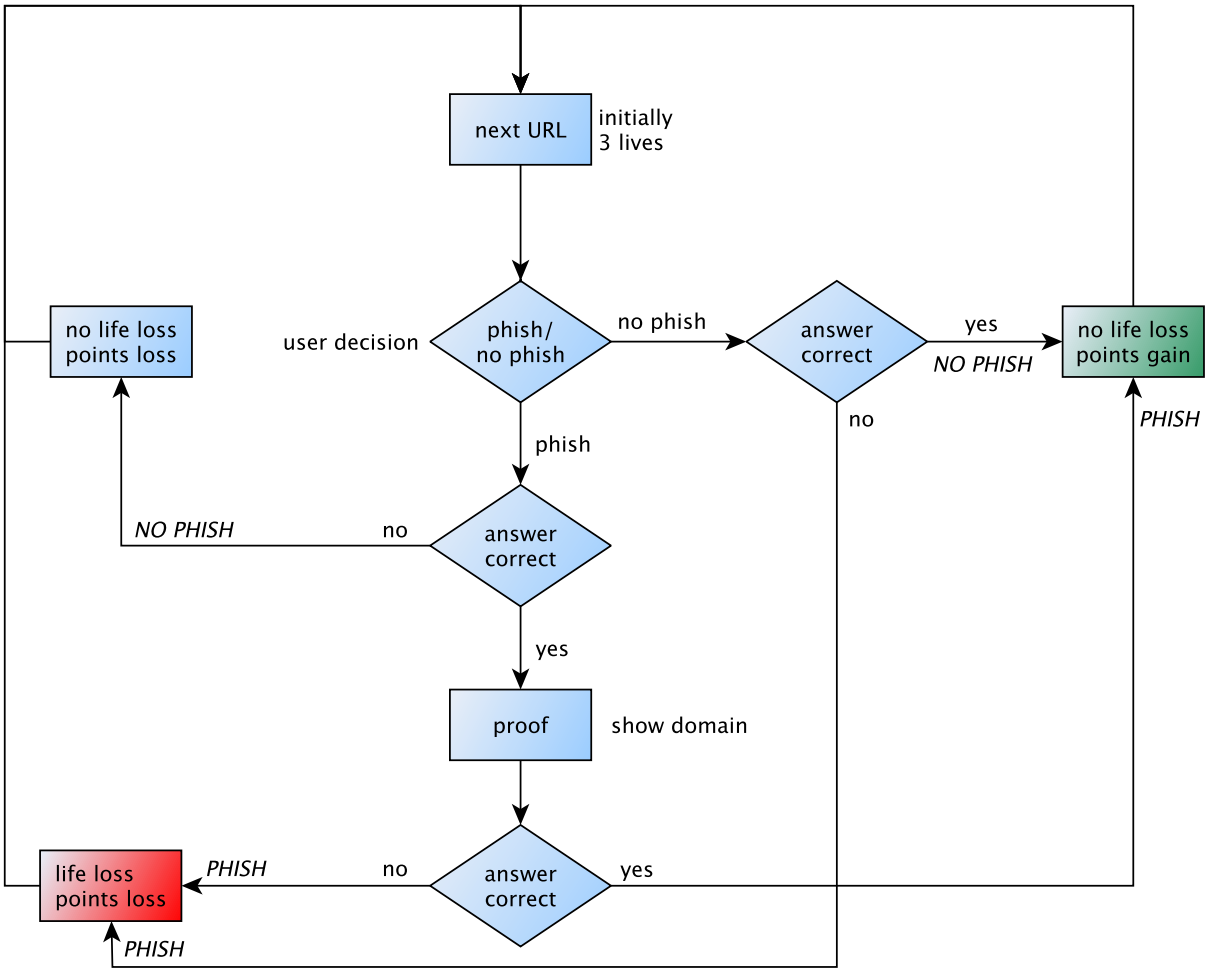


Figure 12: Losing points and lives in the game (levels 2-8). PHISH/NO PHISH refers to whether the displayed URL is a phish or not. In case the terms are not capitalized, i.e. phish/no phish, they refer to the user's decision.

Level 1: The actual game starts with level 1, where the user learns about the structure of a URL. First of all, the user gets an overview of the single components of a URL. In order to make the these components easier to understand we used an analogy which is summarized in Figure 13 with an example URL. We told the user that he has to imagine that the website he is visiting is his communication partner. Furthermore, the user is told that the section between "http(s)://" and the third slash "/", i.e. the hostname, reveals information about his communication partner. In particular, we explain that he has to read this part from right to left. The domain of a URL is introduced as "Who-Section" (company + location of the company), from which the user knows who he is actually talking to. All other parts in the host area are to be considered as "departments" of the company of ther user's comminication partner. The protocol part is introduced as "Security Level" of the conversation with the partner and the path part of a URL, i.e. the part after the third slash "/", is introduced as the topic of the conversation with the communication partner. When marking parts of a URL we consistently used the according colours of Figure 13. The task of level 1 is to identify the domains, i.e. the "Who-Section", of some valid URLs.

Level 2: With level two we start introducing the spoofing tricks of a phisher. We considered the subdomain attack, cf. section 7.4.1, as a good starting point to introduce the phisher as the user has just learned about the importance of the "Who-Section" in level 1.

Level 3: In level 3 the user is first told what an IP address is. To facilitate the comprehensibility, we used the analogy of house addresses. The user is explained that like addressing our houses with street names and numbers, computers in the Internet are addressed by so called IP addresses. The IP address itself is defined as a 4-place sequence of numbers, separated by dots. Finally, the user is warned against URLs with IP addresses in the host part.

Level 4: In this level we deal with nonsense in the domain, cf. section 7.4.1.

Level 5: In this level we deal with domain names which sound trustworthy, but are in fact unrelated to the company name, cf. section 7.4.1.

Level 6: Here, misleading and deceiving names in the domain of a URL are covered. This includes typos, scrambled letters or other similar and deceptive names in the second-level domain, cf. section 7.4.1.

Level 7: In this level we focus on homograph attacks where the user is able to visually distinguish a fake domain from the original one, cf. section 7.4.1.

Level 8: In this level the user is introduced to an attack where the brand name of the visited website or even the whole legitimate URL is placed in the path of a fake URL, cf. section 7.4.1.

Level 9: Here we introduce the difference between HTTP and HTTPS. In particular, the user is told that the usage of HTTPS means that his conversation with the website is encrypted and that the communication partner indicated in the "Who-Section" is authenticated. As an analogy we say that the HTTPS represents the higher security level of the conversation. This means, the conversation cannot be eavesdroppbed by an attacker and the communication partner indictated in the "Who-Section" has proved his identity to a trusted third party. With HTTP this security level is not established. In this level the user is generally required to reject HTTP URLs. On HTTPS URLs the user has to validate whether they are legitimate or phishes.

Level 10: This level does not include an exercise. It mainly serves as a section with some important additional input for the user. Specifically, we tell the user two things: First, we explain to him that he might encounter URLs which actually look very fraudulent (cf. section 7.4.2). In such a case, we suggest to directly contact the company and ask for the authenticity of the specific website before entering any data. Furthermore, we introduce extended validation certificates. We provide the user with a link to further information to this subject.

Figure 13: URL components that are communicated to the user

8.5 Leveling Strategy

During the app development we examined several strategies on how to gain points and setting thresholds for unlocking the next level and incrementally improved it. This section is intended to introduce the leveling strategies we considered for the app together with an assessment of their strengths and weaknesses. Finally, we describe the strategy we chose to use.

Leveling Based on Achieved Points: Our very first leveling strategy was based on the achieved points per level. On each level the user had to achieve 100 points to pass the current level and unlock the next one. This approach had a major drawback. The fact that achieving a minimum of points to pass the level results obviously in very similar points for everybody finishing a specific level. That is to say, the comparison between single users would not be meaningful as the points would only differ very slightly. Additionally, users gain points for each run of a level. Therefore, given the fixed amount of points to be achieved, users might replay early levels which are easier and gain the same or even more points compared to users playing later and more difficult levels.

Leveling Based on Detected Phishes: The previously described leveling strategy had the deficit of comparability among the users. However, we consider comparability very important since it serves as an incentive for the user to perform better or play on. For this reason, we decided that passing a level should rather depend on the number of phishes the user was able to detect during a level. That is to say, in every level there is a certain amount of phishes the user has to detect in order to complete it. With this approach there is still the possibility for a user to repeat early, and thus easy, levels and possibly gain more points than users playing later, and thus more difficult, levels. To prohibit this, in increasing levels the users gains and loses increasing points accordingly such that it does not pay off to replay lower levels. The points for each answer p in each level n is modified by the following formular:

$$p * 1.5^n$$

This strategy solved the problems of our first strategy, however it also brought a new one: always rejecting a URL will eventually result in passing the level (if the user also correctly identifies the domain when required). Such a downside is suboptimal for a game.

Leveling Based on Correct Answers: To solve the problem of our second leveling approach we extended the leveling passing to correct answers. Instead of detecting a certain amount of phishes per level, the user has to give correct answers to a predefined amount of phishing URLs as well as a predefined amount of valid URLs in order to pass a level. Only and only if the user correctly answered the predefined number of valid and phishing URLs the level is completed. To additionally incentivize the users we included three lives per level. The lives are supposed to prevent a user from playing eternally, without ever passing the current level. In case the user loses all of his lives, cf. Figure 12, this indicates that he did not understand what the level was about. Therefore, he has to restart the level. He is returnt to the introductory block of the level he just lost. The points are assigned exactly as before. This is our final leveling strategy for the app.

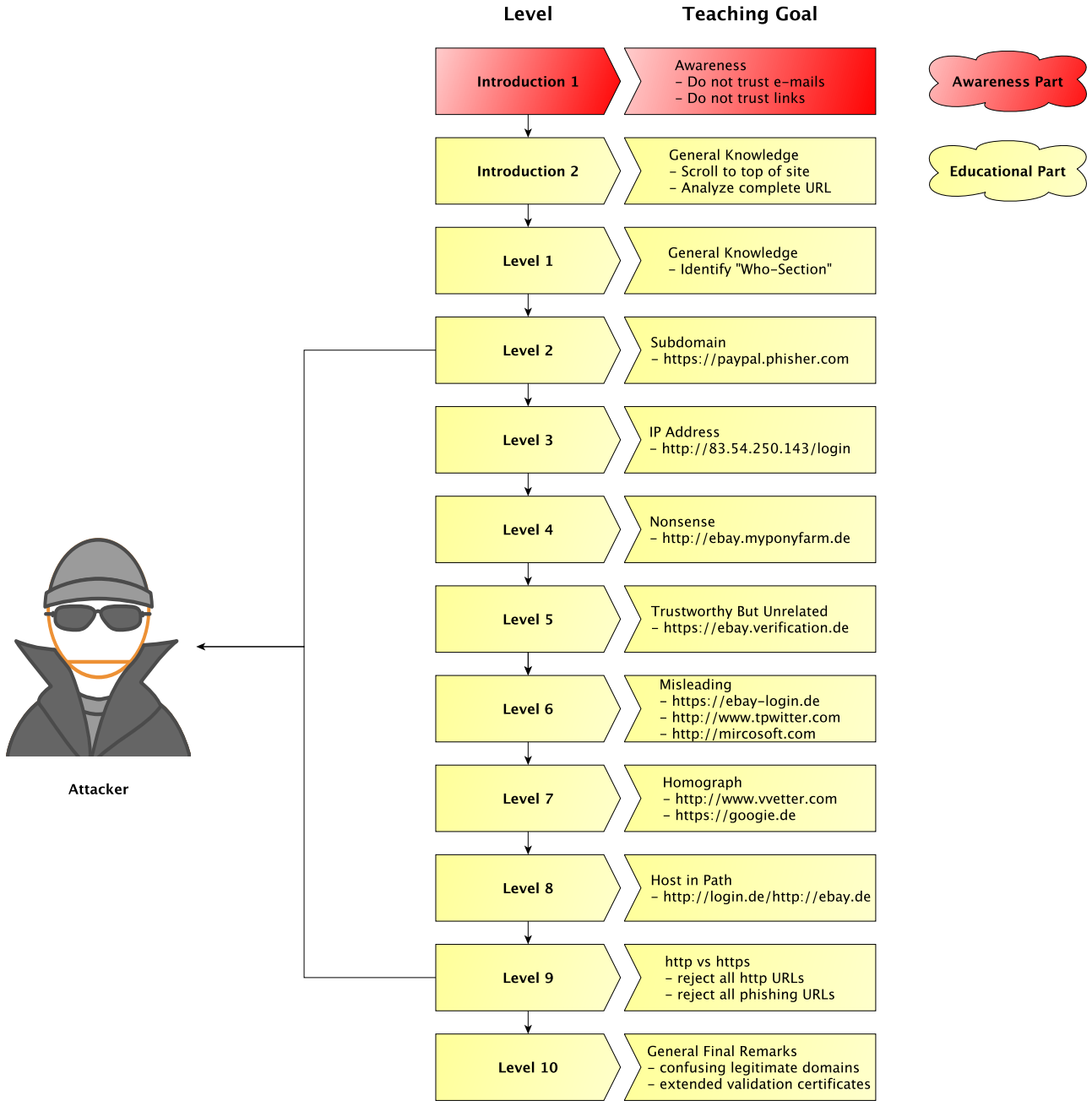


Figure 14: Teaching goals per level

8.6 Use of Learning Principles and Game Techniques

Our app is a learning game which purposes to introduce information on the topic of phishing and how to detect it. With the app we want to improve understanding for this topic and help users be less vulnerable for falling for such attacks in future. This section deals with the principles of learning and game techniques which are reflected in our app design. In fact, the laws of learning and game techniques have a strong connection which is the reason why games work for learning purposes [69].

8.6.1 Principles of Learning

Edward Thorndike introduced the first three principles of learning: readiness, exercise and effect [70, 69, 71]. Later the principles of learning were further extended by: primacy, intensity and recency [69, 71]. These principles outline how people learn and which conditions improve their process of learning. In the following we will briefly introduce the meaning of these principles [69] and explain how they are reflected in our app.

Readiness: The principle of readiness claims that physical, mental as well as emotional preparedness is an important prerequisite for a better learning performance. It also states that motivation is crucial for effective learning. First of all, students must want to learn something, otherwise any additional motivational efforts will be of no use. In order to make students want to learn something it is relevant for them to see a clear reason for learning, i.e. the perceived value of the material is ultimately related to their motivation. Finally, the principle of readiness says that best learning performances are achieved in combination with good physical health. The physical and health conditions of our app users are beyond our control. For this reason this is an aspect which cannot be reflected in our app. The app is targeted at users who are willing to learn something about phishing. Consequently, there is already some kind of motivation in our app users. In order to increase this motivation we present clear reasons why the user should continue to play our app. This is happening in the awareness part, where the user is told what exactly phishing is, how easy it is to phish users, spoof e-mail senders and content, spoof links as well as create exact copies of legitimate websites, cf. section 8.1.

Exercise: The use of exercise is composed of two important parts: First, training and repetition help increase learning. Second, feedback is crucial for good learning performance. For best learning results, these two parts must be applied together. In a nutshell, the learning connection is strengthened by practice, and weakend by disuse [71]. After finishing the awareness part, we start with the user education and provide exercises for all of our learning goals (except for the last level), cf. section 8.4. The learning content is also permanently repeated. For example, in the introduction 2, cf. section 8.4 the user learns to scroll up to make the address bar re-appear and analyze the URL by right and left scrolling it. The scrolling of the URL is present in levels 2-9. Also, the user has to identify the Who-Section in level 1. In addition, the user has to show the Who-Section every time he has detected a phishing URL correctly. Finally, every introduced attack of each level n will appear in level n+1 at least once. That is to say, as soon as the user gets to know a new attack, he will keep seeing this attack in the succeeding levels. Our app also provides direct feedback to the users' actions. In case of correct answers, the user is rewarded with gained points, with a smiley and a small text that he has done well. When the user has made a mistake he is punished with losing points, possible life loss and a sad smiley. Also, the user is told that the answer was wrong, why it was wrong and additionally he gets a reminder text on the applied URL spoofing attack he was not able to recognize. To sum it up, we let our app users practice what we taught them and make use of repetitions in combination with direct feedback.

Effect: A student who associates his learning with positive feelings will learn more and better than another student who connects his learning with negative feelings. For example, a student who is unsuccessful with initial learning material will associate his experience with unpleasantness, frustration, anger and/or confusion, while a student with early success will have strong positive feelings and thus will be more motivated to have more success in future. Therefore, enabling particularly early success and maintaining student motivation with positive feedback and comments is crucial. In our app early success is easy to achieve, since we start with easy tasks and obvious attacks which get increasingly difficult in higher levels. When the user has given a correct answer he is rewarded with a big smiley face as well as points. Also, the user is shown a medal every time he finishes a level. These aspects of the app are intended to increase the users'

positive feelings and keep him motivated to go on. However, some improvement of positive comments might be worth considering. Currently, the positive texts for a correctly answered text, for finishing a level and icons do not differ. It might be more engaging if such texts and icons differ from time to time in order to increase the positive emotions of the user. For example, texts telling the user that he has done well might slightly vary (for instance, according to the degree of difficulty of the achieved task). Also, the screen of finishing a level could vary. Here again the degree of difficulty might be considered. According to the level finished, the obtained award could get bigger, the text of the level finished screen more flattering in order to increase the users positive experience.

Intensity: This principle says that learning is better encouraged by things that are more intense. For example, people likely to learn more from an exciting and enthusiastic teacher than from a boring and monotone one or from a text book. Our app is by nature more intense than a simple text based approach. The game creates incentives and intensity. Also, the fact that we do not only tell the user that e-mail spoofing and link spoofing is easy but also make him experience it increases the intensity.

Primacy: The principle of primacy means that the first thing a student learns makes the strongest impression. For this reason getting rid of bad habits, and replacing incorrect or wrong logic are difficult. This principle is coupled with time. The first things our users learn is: what is phishing as well as how easy e-mail and link spoofing is. For those who already knew these things, the awareness part will not be such a high motivating factor. Yet, we believe this part is indispensable since there are still many people outside who are not aware of the aspects mentioned above.

Recency: The principle of recency states that most recently learned things are easier to remember. This is a consequence of the reduction of the learning over time. The principle of recency is coupled with time. We are aware that our app is not a game which will be frequently used and thus its users are likely to forget the content they have learned, for example, a week ago. In order to overcome this problem, so called reminders are included in each new level introduction. An example view of these reminders is depicted in Figure 15. There the user has a short summary of what he has learned so far. Also, we keep confronting the user with attacks from previous levels during the exercise rounds. This repetition is, on one hand, intended to strengthen the users knowledge and understanding, on the other hand, it is intended to create a kind of recency so the user does not forget about this kind of attack. In case the user does not detect the attack (a repeated or a new one) he will be reminded what kind of attack had been applied. Furthermore, in this level the user will be confronted with this kind of attack again, until he gives a correct answer to it.

Now that we have introduced the fundamental principles of learning and associated these with our app, we proceed with the introduction of game techniques and how they are related to the learning principles as well as to our app. As already mentioned, there are strong connections between learning principles and game techniques. Therefore, we will try not to focus on redundant aspects, but rather on additional aspects which need to be considered in game design.

8.6.2 Game Techniques

Basic game techniques are: flow, feedback, simplicity, immersion and engagement, choice and involvement, practice as well as fun [69]. As some terms already reveal, these principles are strongly connected to the basic principles of learning. In the following we will elaborate on these game techniques by stating their relation to the according learning principle, mentioning additional aspects to consider and how these are mirrored in our app.

Flow: Flow is the key point of games. It is “the state in which people are so involved in an activity that nothing else seems to matter; the experience itself is so enjoyable that people will do it even at great cost, for the sheer sake of doing it” [72]. Sometimes flow is also referred to as ’engagement’ [69] and relates to a person’s overall well-being [73]. Flow relates to motivation [72, 74]. Motivation in turn is a crucial part of readiness, cf. section 8.6.1. In essence, there are four requirements for flow [72, 74, 75].

1. *Clear Tasks:* With clear tasks the user is able to understand what he needs to do. The tasks which need to be completed by the users of our app are never complex and they are always clearly told what they need to do next.

2. *Feedback:* With feedback the user should always be kept up-to-date about his progression towards the goals he is asked to achieve. He also should get immediate feedback on whether his actions are good or not. Our app covers these aspects, cf. section 8.6.1.
3. *Balanced, Attainable Goals:* The user should be confronted with challenging tasks, but at the same time these tasks should also be achievable. Especially in the beginning our app users are confronted with very simple tasks. For some users they even might be too easy which may result in a loss of interest. However, these tasks are important basics which are necessary for successful detection of phishing attacks on the smartphone. Therefore, for future work especially the first two tasks (access address bar and analyze the complete URL) could be re-designed so that they also keep users which have already knowledge in this area. Currently, the users can just skip the introductory part of this part and directly complete the task. Besides, as the users' skills will naturally improve, their tasks get more difficult and challenging with increasing levels, but will remain achievable.
4. *Concentration:* The user should not be distracted with, for example, complex interfaces. He should rather be able to fully concentrate on the game. Our app has a very simple user interface with the most necessary elements. There are no special effects, advertisement or other elements which might distract the user from playing the game with full concentration. The only intrusive and interruptive elements are our introductory sections. However, these are inevitable for the communication of the learning content.

Feedback: Feedback is important which is also reflected by the fact that it is a crucial part of the learning principle 'exercise', cf. section 8.6.1, as well as a requirement for flow. Stated simply, feedback is how a user perceives progress [72, 74]. For the completion of even simple tasks feedback is indispensable. Feedback can be in form of a scoring system, comparative statistics or failure outcomes and provides the user information about his progression and performance. Games make use of a so called feedback loop [76]:

1. *Measure Behavior:* Our app assesses whether the answer of the user to a given task is correct.
2. *Relay Measurement to User:* The user is told whether his answer is correct or not.
3. *Realize Some Sort of Outcome:* The outcome of the users' actions and answers are accordingly defined, cf. section 8.3. For example, the user loses a life in case he did not detect a phishing URL.
4. *Provide Opportunities for Alternate Action:* The user has the chance to do better in the next tasks.

Simplicity: The real world is a complex construct. However, games should simplify the real world so that there only remain rules and goals. In this way the players can fully concentrate on their tasks and how they can achieve them [74]. Hence, simplicity helps users to achieve flow and thus increased motivation. This, in turn, leads to improved learning, cf. section 8.6.1. Simplicity involves, for example, the user interface, the game goals, feedback loops, rules and instructions. The structure of our app is kept simple and consistent. Therefore, it should be easy to understand. Our user interface is kept to the necessary minimum and the goal of the game is clear: detect phishing URLs.

Immersion and Engagement: Immersion involves a passive activity. The term is used, for example, to describe a person who shows strong interest for a story [77]. In contrast to immersion, engagement involves active actions, such as trying to solve a problem or puzzle. Games commonly use both, immersion and engagement. To achieve immersion game designers make use of stories, visual and audio techniques, attractive graphics or animations [75]. Simultaneously, the user is engaged with choices, problems, or puzzles which have to be solved. The combination of immersion and engagement has the potential of creating an intense game experience [69]. These two aspects of game techniques are strongly linked to the learning principle of intensity. By challenging the user with various tasks to solve we meet the requirement for achieving engagement. However, immersion is an aspect we have not considered yet within the scope of this thesis. In order to achieve an intense game experience, this aspect might be worth considering for future work.

Choice and Involvement: Games consist of choices and involvement. There is a link between choice and positive feelings (cf. Principle of Effect in section 8.6.1), i.e. choice is important for a person's overall well-being [73, 78]. However, the downside of choices is the so called paradox of choice which states that choice is beneficial, but too many choices

can cause more bad than good [78]. The problem is, when the users are confronted with too many choices they get overwhelmed, since the decision thus the task to solve becomes too complex. We believe that our app does not face the problem of this paradox since the decisions the user has to take are limited to the questions: is the following URL a phish, and show us the Who-Section. Still, the user has to make decisions and is consequently involved in the game.

Practice: This technique is directly related to the learning principle of exercise, cf. section 8.6.1. Users practice and repeat several steps of games extensively so that they eventually gain mastery and the difficulty of their challenges can increaseč itemurphy2011games,schell2008art. Our app offers practices as well as repetition, cf. section 8.6.1.

Fun: Fun is an important aspect of game design and yet the definition of it is not clearcut in literature [69, 75, 79]. Based on several definitions found in literature Curtiss Murphy introduced the following definition of fun: *"Fun is the positive feelings that occur before, during, and after a compelling flow experience"* [69]. Positive feelings include, but are not limited to, engagement, enjoyment, pleasure, entertainment, satisfaction, control and triumph. Fun is related to the learning principle of effect and its positive feelings. How we achieve the principle of effect and positive feelings in our app is described in section 8.6.1. Yet, fun is something which emerges from several game techniques, such as, flow, immersion and engagement, practice to achieve mastery, and choices, which all lead to positive emotions. Fun is an aspect of our app which could be considered more deeply in future work. Especially, the areas of creating positive feelings and including immersion in order to make the users' game experience more intense and fun are aspects which might be looked at.

9 App Development Process

This chapter summarizes important steps concerning the development process of our app. We do not provide in-depth insight to our implementation. Instead we give a brief overview of our approach for the development of a user friendly and understandable app.

9.1 Mock Up

After we decided about the work flow and structure of our app we built a mock up in order to get a more concrete idea of what needs to be implemented and to reveal flaws in our thought process. We showed it to friends and relatives so we could expose aspects we have not yet thought about. The first texts explaining how to access the address bar and the structure of a URL seemed to be difficult to understand. As a consequence, we adjusted these texts in the app (only those of the first three levels) and showed them to other friends and relatives who seemed to understand the descriptions. Based on these initial texts we wrote all remaining texts without including it into the app yet. The next section describes the elaboration process of these texts.

9.2 Pilot Study of App Texts

After finishing the texts for each step of the app flow (the texts were not directly included into the app) our supervisor, a professor of pedagogy at TU Darmstadt as well as another highschool teacher of German reviewed them. Once we achieved the version with which we were satisfied we applied a user study on it. For time reasons, we decided to go for the low cost method of guerilla user testing [80, 81]. This approach enables to quickly assess the effectivity of a design, in our case our app texts. Guerilla user tests is rather loosely structured and do not include participant recruitment. The testers are rather approached, in our case, we asked relatives and friends. The outcome of such studies is rather qualitative, i.e. extensive and detailed insights are achieved. A downside of guerilla testing is that the approached participants might not belong to the defined target group with respect to their expertise or skills. Since we knew our participants we addressed only those who matched our target audience. In detail, our approach for the guerilla user test was as follows:

1. *Preparation of Texts:* Our aim for this user test was to imitate the use of a smartphone as best as possible. For this reason, the app texts were formatted into short lines, so that the text appearance resembled that of a smartphone screen. Furthermore, we printed out the texts and cut the sheets into small rectangles.

2. *Think Aloud:* We asked the participants to think aloud during the test. We told them that there are no stupid questions or comments and that they help most with just saying what goes through their mind. We made notes of their remarks.

3. *User Test with In-Between Exercises:* The actual user test mainly consisted of reading our app texts and thinking aloud about these. We included a little simulation of our exercise parts in order to validate whether the users comprehended the texts or not. For example, for each introduced attack we included a small list of URLs on which the users had to decide whether they were phishing URLs or not.

4. *Final Comments:* After going through the texts the users were asked to provide their general impression. We further asked them about some aspects we were not quite sure about at the beginning. For example, we asked them whether the usage of the terms “link” or “web address” confused them, which was not the case.

Our guerilla user tests showed that our texts are understandable. According to our participants the main downside of the texts was their length. Yet, this can be neglected since the users had to read our complete texts (instead of for example just playing 1-2 levels at once). Furthermore, they remarked that the introduction on how to access the whole address bar and analyze the complete URL is unnecessary. For some users this might apply. However, it is possible that there are users who do not know this. For those who already know how to access the address bar and analyze the complete URL we added a button which directly links to the exercise. In case the user had overestimated himself, he will be forwarded

back to the app, where the introductory text can be consulted. Finally, the provided brief summary of already passed lessons (reminder texts) received some criticism for their frequent re-appearance at the beginning of each level. This can also be neglected since we assume that our app users will not constantly play this game and in our view repetitive serving of the major lessons learned is helpful to internalize them (cf. Principle of Exercise in section 8.6.1). Also, when playing the app this screen can easily be skipped as it exhibits a recognition value achieved by the title “reminder”. Moreover, we decided for a minor reorganization of the reminder view. Before the user tests the reminders mainly referred to the URL structuring they have learned so far. We thought it is also important to remind the users of possible attacks. Therefore, the reminder concerning the URL structure was kept to a minimum with the aid of a graphic. Plus, for each attack in previous levels one sentence and one example was added. To sum it up, the introductory blocks that introduce spoofing techniques of phishers (level 2-9) are generally structured as follows: First, we provide the major lessons learned from the previous levels in the reminder. An example reminder view of level 3 is depicted in cf. Figure 15. Next, a brief introduction to the current level’s topic follows. Finally, the new attack is introduced which includes one or more examples. An example of this view is shown in Figure 16.

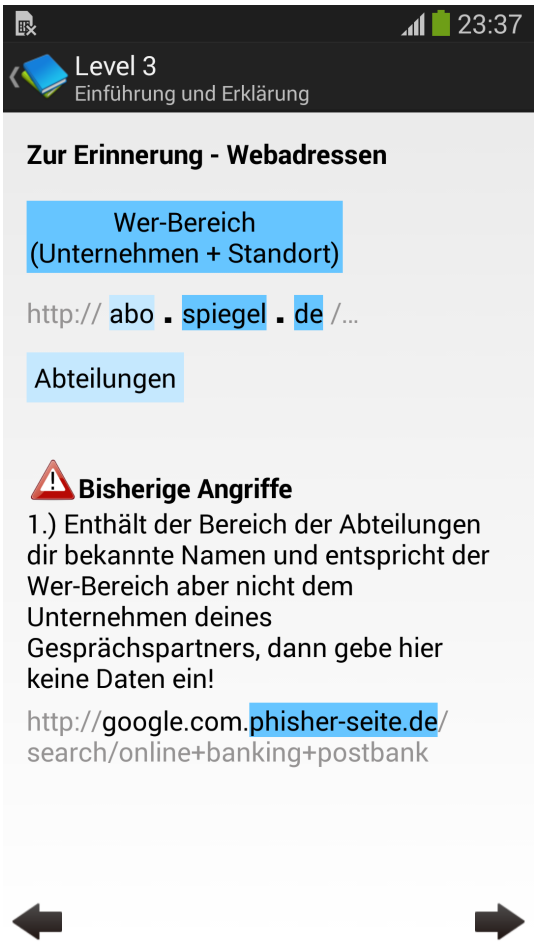


Figure 15: Example reminder view of level 3

9.3 Legibility Index of Our Texts

Comprehensibility is of major importance for our app. Each level starts with a lesson on a certain way phishers make use of in order to delude people. These lessons aim to educate the user by describing those phishing attempts. Hence, it is of utter importance that our explanations are both thorough as well as comprehensible. After we had conducted user tests and included their corresponding valuable feedback (cf.section 9.2) and also received good feedback from the final study (cf. section 10.5.3), we now want to assess the comprehensibility of our texts with the aid of a statistical method. Several approaches to assess the readability of a given text exist [82, 83]. These approaches consider, among

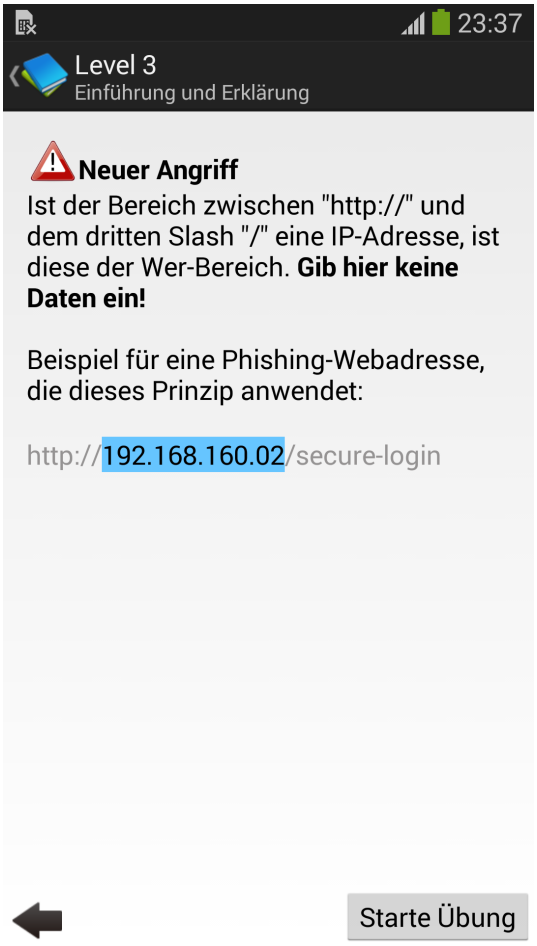


Figure 16: Example view of new attack in level 3

other details, the average word and sentence length and therefore are language dependent and usually are designed for the English language. However, the Flesch-Reading-Ease [83] is a legibility metric that outputs a numeric indication for the readability of the input text and was also adjusted to operate with the German language by Toni Amstad [84]. The readability of a German text is computed as follows, where ASL represents the average sentence length and ASW the average number of syllables per word:

$$\text{FRE}_{\text{German}} = 180 - \text{ASL} - (58.5 \times \text{ASW})$$

Several auxiliary tools exist that take a regular text as their input and return a legibility index as their output [85, 86, 87]. All of these tools delivered different scores because they obviously had varying algorithms to determine syllables, sentences and even word boundaries. Therefore, we approached as follows: First, we took the explanation part of each level as the input for all of the three tools. Second, we extracted the amount of sentences, words, and syllables from the returned values, as depicted in Table 2. We did not rely on the returned legibility indexes, because the tools seemed to use slightly different formulas. Third, with the extracted information we were able to compute the German FRE index ourselves in a consistent way through all of the three tools. Ultimately, we derived a final index value of 62 by averaging the resulting index values of each tool. Given a scale from 0 to 100, where an index of up to 30 indicates an academic level and 90 and above is considered easy to understand, an index of 62 is considered as reasonably comprehensive for teenagers [84]. Regarding our target group, this is a good result and confirms the comprehensibility of our explanations also statistically.

	Leichtlesbar.ch	**Stilversprechend.de**	**Fleschindex.de**
# Sentences	426	604	400
# Words	4616	4760	4762
# Syllables	8305	8658	9235
Legibility Index	64	66	55

Table 2: Sentences, words and syllables of our texts outputted by different tools [85, 86, 87]

9.4 Implementation and Testing

In parallel to formulating and validating our app texts we developed the basic structure and logic of our app. After conducting and assessing the guerilla user tests of our texts and integrating the feedback, we started to include them into our app. We both developed and tested the app simultanously. Occasionally, we showed the app to friends and relatives in order to get some feedback on aspects we might have missed. In this way, our app was formed incrementally. We do not intend to provide implementation details in this work. The only exception is the algorithm used to generate the URLs on which the users have to decide whether they are phishing URLs or not. This approach can be consulted in Appendix B.

10 App Evaluation

After having designed and implemented the app, the evaluation of our work remains as a final step. This chapter describes our evaluation process. The app will be evaluated with the aid of a user study. After introducing our study design, we will state our hypotheses and explain how we are going to measure our statements. Finally, we will analyze our results and state our conclusion.

10.1 Participant Recruitment

This section deals with the participant recruitment for the user study. As an incentive to attend our user study a gift card was raffled among 4 users. A major challenge was not to address close friends in order to receive unbiased and honest feedback. To reach potential participants we proceeded as follows:

Flyer: We prepared a flyer with the most important information. In this flyer we told the user that a learning app about Internet security in general will be tested. We did not mention the specific topic of phishing in advance because we did not want potential participants to read up about it before the study. Copies of this flyer were hung on blackboards of student dorms and some other buildings at the university.

E-Mail to Professors: We additionally distributed the flyer to a number of professors in our university and asked them to forward it to their students and/or teaching staff. We did not forward the flyer to computer science professors or professors of similar technical majors since their students and staff most likely do not match our target group.

Online Social Networks: We contacted our friends in online social networks and asked them to ask friends whether they would be willing to participate in our user study. Additionally, we posted the flyer in university groups of online social networks with the hope some people might be interested in participating.

Further Networks: Finally, we called friends we could not reach via online social networks and asked them if they knew anybody who would participate.

In section D.1 copies of our e-mails to the professors and of our flyer can be consulted. Note that we had to split the user study into groups of 4 participants due to the lack of available smartphones. Moreover, our flyer originally said that the best participant of each group would win the gift certificate. However, we recognized that the winning chance might not be equal for every participant due to varying expertise, for example, or other possible technical problems such as app crashes. For this reason we asked the participants at the beginnig of each study whether they agreed to raffle the gift certificate instead. To express our appreciation to each participant we decided to offer cookies and other kinds of sweets. Additionally, the participant who performed best was awarded with a “Golden Anti-Phish Certificate”, all other participants received a “Silver Anti-Phish Certificate” (cf. section D.4).

10.2 Study Design

For our user study we chose a within-subject design, i.e. a “before and after app” study with the same group of people. The advantages of this design can be summarized as follows: Within-subject deals better with variability associated with individual differences compared to between-group design, where different groups would be considered who do and do not play the app. A major drawback of the within-subject design, however, is the learning effect. We are not able to clearly distinguish whether a behavior change after playing the app is a result of the app intervention or of learning effects. Yet, our results showed that the learning effects seemed to have only a minor impact (cf. section 10.5.2).

Figure 17 illustrates the structure and process of our study. In the following, we dwell on each of the consecutive steps:

1. *Informed Consent:* Before starting the user study the participants have to sign an informed consent. This form briefly explains what the study is about and clarifies that the participant is not obliged to finish the study. If the user terminates the study before finishing it, however, he cannot participate in the gift certificate raffle. Optionally, the user can agree with the anonymous publication of the:

a) transcriptions of the study (recordings will be deleted after the study)

b) filled out surveys

2. *General-Survey Before:* At the beginning the participants have to fill out a general survey, where they have to judge their own knowledge on the topic of Internet security in general. For instance, they are asked whether it is easy for them to distinguish legitimate e-mails and websites from fake ones.

3. *Website-Survery Before:* In this part of the user study the participants get a list of screenshots of websites. The screenshots had been taken with the standard browser of an Android tablet. In total, the user is shown 16 screenshots, with 8 phishing and 8 valid URLs. The user has to decide whether he would enter confidential data on the shown website. Additionally, he has to encircle the part of the screenshot which was the primary reason for his decision. Then, the user has to indicate how sure he was about his answers on a Likert scale. Finally, the user is asked whether he knows the vendor of the website and whether he has an account there. The list of the used URLs can be found in section D.3.1. Note that we used the same order for every participant's survey, i.e. everybody was confronted with these URLs in the same order.

4. *Play App:* Here, the users get the smartphones in order to play the app. To save time, we skipped the introduction 2 part (how to access the address bar) for the user study. The user has half an hour to play. Afterwards, they are asked to put the smartphones aside. Then, we collect the smartphones and note the reached points for each level. Note that the selection of URLs in our app is randomized. This means that the users were confronted with random and thus possibly different URLs.

5. *Website-Survery After:* After playing the app, the participants get a second website-survey. In this, all examples of the previous survey are included. Moreover, it contains 8 further website screenshots of which 4 represent phishing and the other 4 legitimate URLs. The list of the used URLs can be found in section D.3.2. Note that we used the same order for every participant's survey, i.e. everybody was confronted with these URLs in the same order.

6. *General-Survey After:* Here, the participants are asked to complete a form with questions pertaining to their person, for example, their age or course of study. This form does also contain questions related to the System Usability Scale (SUS) [88], which is supposed to assess the usability of our app, and questions regarding the users' impression of the app.

7. *Certificates:* At this point the official part of the study is finished. We thank the users for their participation and award a "Golden Anti-Phish Certicate" to the best participant of the current group. All other attendants receieve a "Silver Anti-Phish Certificate". Next, the gift certificate is raffled.

8. *Debriefing:* After the official end of the study (after handing out the certificates) we asked the participants if they were willing to stay for an optional debriefing, where they could ask questions or provide their remarks in person. In case a participant did not want to stay for this debriefing, he was free to go.

10.3 Hypotheses

In order to evaluate the effectiveness and usability of our app we formulated the following hypotheses and measurements.

1. *Hypothesis 1 - Mistakes:* After playing the app, the users make significantly less mistakes when deciding whether a website is a phish or not than before using the app.
   Measurement: Correctly identified websites in "Website-Survery After" (phish or no phish) >> correctly identified websites in "Website-Survery Before"

2. *Hypothesis 2 - URL Based Decision:* After playing the app, the users primarily base their decision whether a website is a phishing website or not significantly more often on the URL compared to before playing the app.
   Measurement: Number of URL markings in "Website-Survery After" >> number of URL markings in "Website-Survery Before"

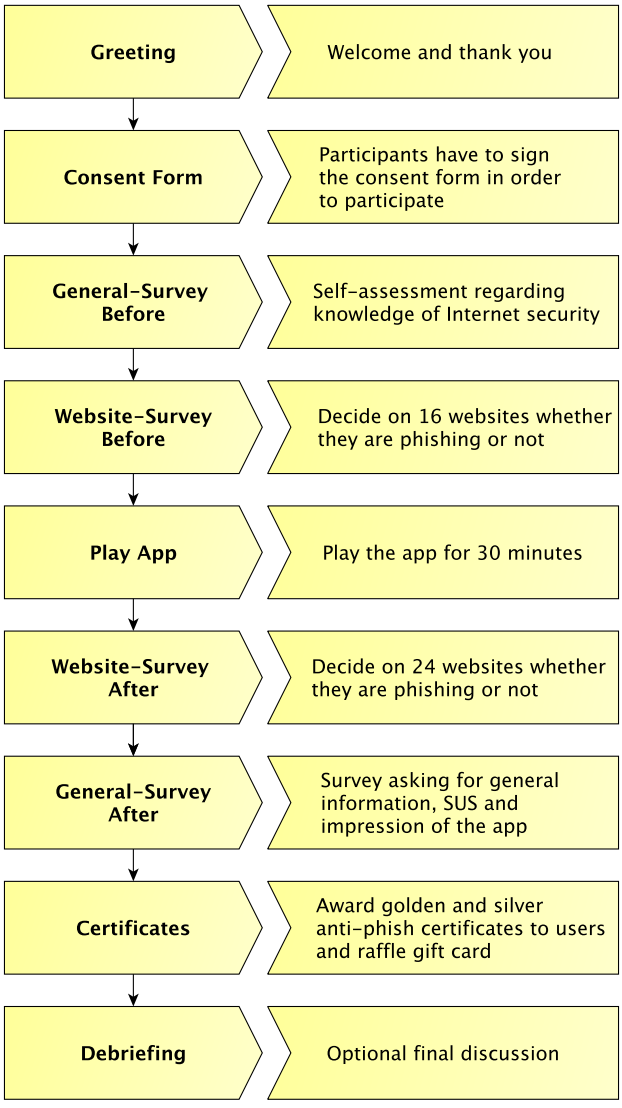


Figure 17: Structure and process of our final user study

3. *Hypothesis 3 - URL Comprehension:* After playing the app the user understands that the domain of a URL is the most important criterion to detect phishing websites
   Measurement: Number of marked URL domains in “Website-Survery After” >> number of marked URL domains in “Website-Survery Before”

4. *Hypothesis 4 - Good Usability:* The usability of the app is above average.
   Measurement: A System Usability Scale (SUS) > 68 can be considered above average usability [88].

10.4 Classifying Markings

One part of the study involved marking the area on a given website which contributed to the users’ decision on whether they thought the website was fraudulent or legitimate. In order to assess these markings, for the measurement of hypothesis 3, we needed to define respective codings. To digitize the markings of the participants we proceeded as follows: One of us read out the markings and the other wrote them down. Occasionally the writing person checked whether he had the same impression. When the reading person was uncertain he also asked the writer. In some very uncertain cases we consulted a third party. Here, we provide an overview of the regions participants marked during the website-surveys and how we coded them internally for the evaluation. Furtheremore, we discuss our marking interpretations and outline several interpretation problems, due to imprecise markings, and how we approached those.

10.4.1 Marking Examples

The following list summarizes the codings we used for the markings of the participants.

1. *None:* Occasionally, participants did not mark or encircle anything of the screenshot. In our raw data this is coded as none (cf. Figure 18).

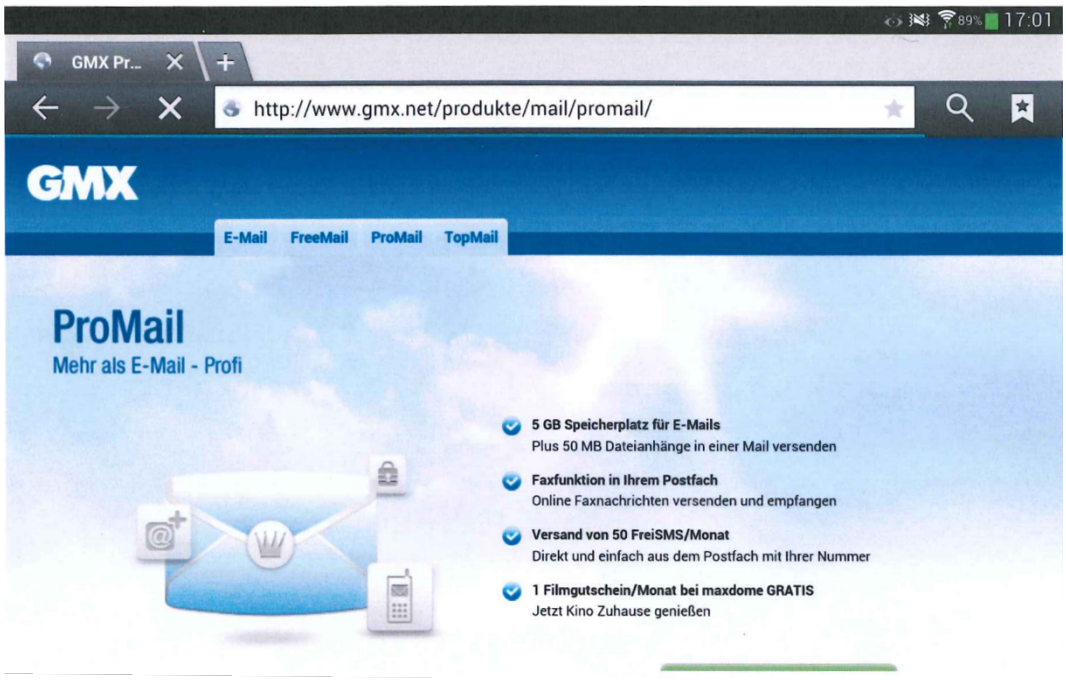


Figure 18: Nothing marked

2. *Favicon or Padlock:* The marking of a favicon or padlock is trivially coded accordingly (cf. Figure 19).

Figure 19: Padlock marked

3. *Content:* If anything else than the URL itself, a part of the URL, a favicon, or a padlock is marked then this is coded as content (cf. Figure 20).

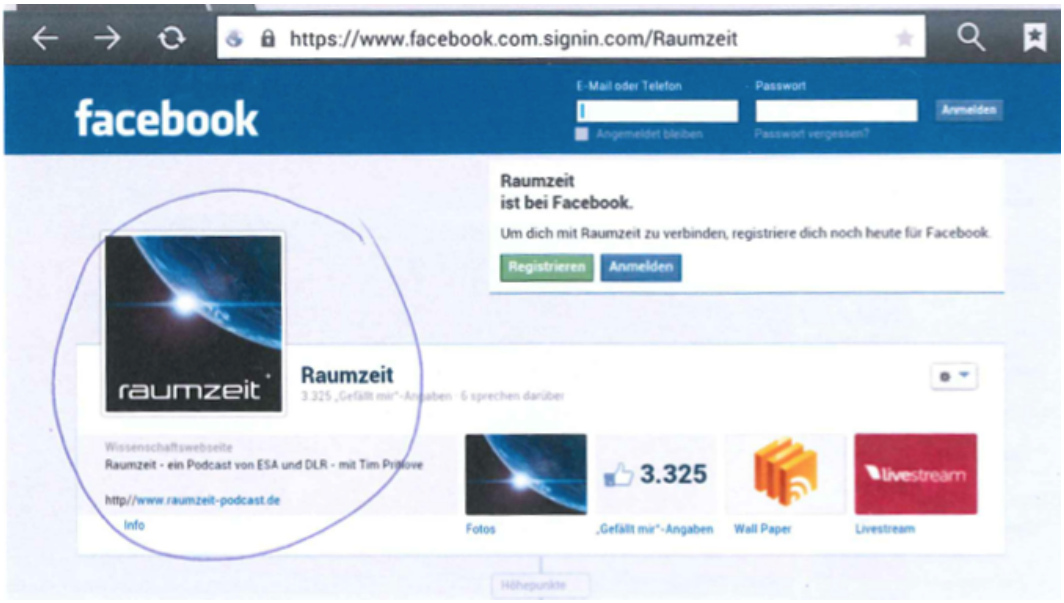


Figure 20: Content marked

4. *Scheme:* If the scheme or a part of the scheme in a URL is marked, this is coded as scheme (cf. Figure 21).

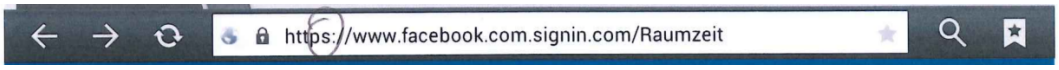


Figure 21: Scheme marked

5. *Host:* Marking the host results in an according coding (cf. Figure 22).

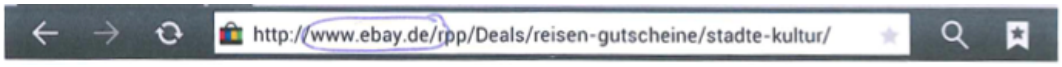


Figure 22: Host marked

6. *Domain:* In case a participant marks a domain (cf. Figure 23) or the substring of a domain (cf. Figure 24) this is coded as domain or domain substring accordingly. For the measurement of hypothesis 3, domain as well as domain substring markings are considered domains.

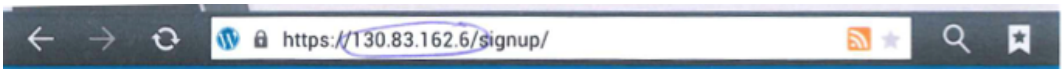


Figure 23: Domain marked

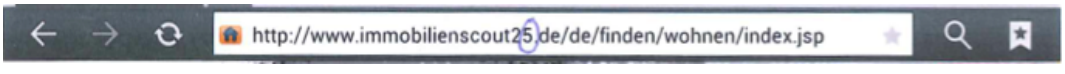


Figure 24: Domain substring marked

7. *URL:* All other markings are coded as URL and measured as such. For instance, the subdomain of a URL is coded as URL (cf. Figure 25).

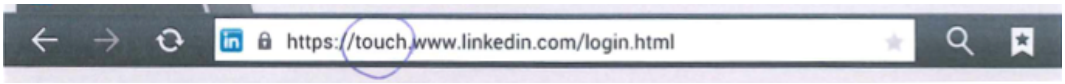


Figure 25: Subdomain marked, coded as URL

10.4.2 Interpretation Problems

While assessing and digitalizing our data we had to face some interpretation problems which we exemplify in the following. In such cases we had no choice but striving to interpret the samples as objectively as possible. Figure 26, for instance, shows a marking where the circle includes the content (YouTube logo) as well as the host. For this sample, we decided to code the marking as host. The next example in Figure 27 shows a marking where a subdomain and the domain is marked. When we faced examples like this we decided to code it as domain in case a subdomain is only partially marked, so that there is an indication that the user just did not make his markings precise enough. If the subdomain is obviously marked deliberately, i.e. clearly inside the circle, this kind of sample is coded as URL. In this case we see that the subdomain is inside the circle and coded this sample as URL accordingly. Another frequently occurring sample is one where two areas are marked, even though we explicitly asked to mark only one. In these cases we decided as follows: in case a marking is obviously striking due to a thicker circle, for instance, the more emphasized area is chosen for coding. In case both markings were equal, we joined the markings and decided based on that. In Figure 28, for instance, a participant marked the scheme and the host separately. We cannot observe any emphasis on one of the markings. Therefore, we chose to code this sample as URL. Finally, there were samples where the user correctly identified a phishing website. However, instead of marking the domain as the reason (as it is done in the app), some users marked the attacked part instead. Figure 29 illustrates such an example. In fact, marking the attacked part is justified. Yet, we had to code such samples as URL since there is no clearcut way of defining whether an attacked part of a URL was recognized or not. In the contrary, the domain of a URL can always be considered as the attacked part. Therefore, users should primarily base their decisions on domains.

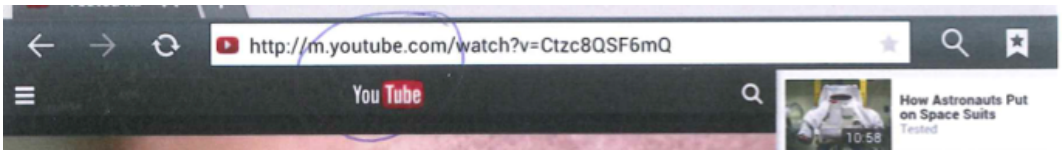


Figure 26: Host or content marked?

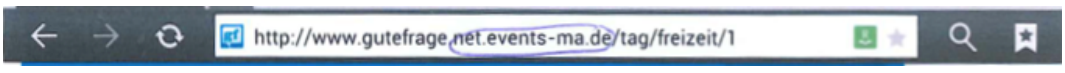


Figure 27: Domain or URL marked?

Figure 28: Scheme or host marked?

Figure 29: Attack marked

10.5 Results and Analysis

This section presents our results and analyzes them. We start with discussing the representativeness of our participants and proceed with illustrating interpretation problems we faced while we assessed the website-surveys. Therafter, we evaluate our hypotheses and proceed with further exploration of our results, followed by discussing the limitations of our study. Finally, this chapter concludes with a disussion of our results and a corresponding summary.

10.5.1 Representativeness of Our Participants

In section 5.1 we defined preconditions that users have to hold in order to match our target group. We aspired to recruit participants who hold these preconditions as far as possible. In the following we discuss the representativeness of our participants with the aid of these preconditions.

Attackability: Generally, we took care that the people we recruited do not have extensive prior knowledge on this topic. For example, our flyer asked for non-specialists. Yet, we were not able to assure beforehand that we would only have non-specialist participants. In such a case we had to rule them out for our analysis afterwards. Unlike in our initial survey (cf. section 6), we did not exclude electrical engineers or computer scientists in general from our final user study. The problem with the phishing survey was that it did not give us enough indication whether a particular participant was too familiar with the topic. Therefore, we had to imply that computer scientists and electrical engineers are too skilled, even if this does not necessarily need to be the case in reality. In fact, there might be computer scientists or electrical engineers who can learn something from our app. In contrast to the phishing survey, in our final user study we were able to determine a user's prior knowledge more precisely with the aid of the website-survey before. Therefore, we did not primarily consider their course of study or field of work, but rather how well they performed in the website-survey before playing the app (cf. section 10.5.2). This way we assured that the considered participants were potential targets of phishing.

Android Users: For the study we considered it important that our participants own a smartphone in general since we wanted the focus to be on our contents. This way, we minimize failures resulting from general operating difficulties. Since we provided the required smartphones during the study we had no need to recruit participants who obligatorily own an Android smartphone. Overall, 7 of 17 participants owned an Android and 10 of them owned an iOS smartphone, i.e. every attendant was a smartphone owner.

Language: Participants of our study need to know German because all of the app texts are in German. This was ensured by providing flyers and e-mails in German language so that persons who do not master the German language do not feel to be addressed. All of our participants could speak and read German.

Motivation: We mainly target users who download our app by choice and thus have a basic motivation to learn something from it. For the user study our flyer was supposed to draw interested persons to participate in our study. Furthermore, we created an additional incentive to attend our study by raffling a gift certificate.

Finally, we aspired to recruit participants who are not close friends of ours in order to minimize biases as far as possible.

10.5.2 Analysis of Our Hypotheses

In total 19 participants attended our study. As discussed in section 10.5.1 we did not exclude any participant beforehand because by means of the website-survey before we were able to precisely determine the prior knowledge of the participants. Ultimately, we had to sort out two participants for the results and analyses of our study:

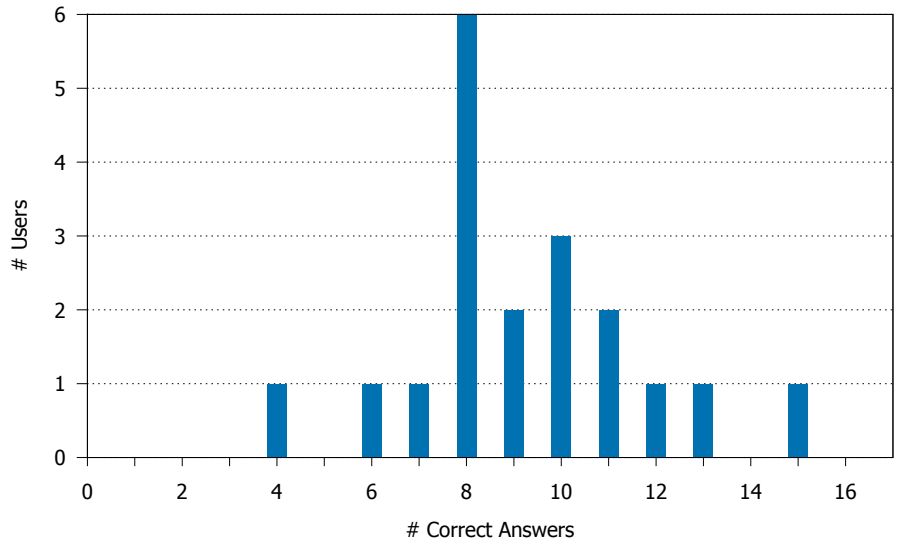


Figure 30: Performance of unfiltered users before playing the app depicting an outlier

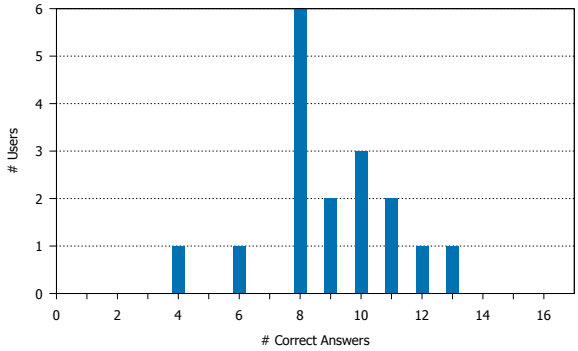
1. *Outlier:* Figure 30 depicts the performance of our participants. It illustrates how many URLs were correctly identified by how many users. Evidently, there is an outlier among our participants. One user gave 15 correct answers to 16 questions. This means that he has too much prior knowledge on this topic and thus does not match our target audience. Therefore, this participant is not considered for our further elaborations.

2. *Seriousness:* Another participant obviously did not engage himself to play our app. During the 30 minutes of playing the app the user managed to complete the awareness part and level 1 (identify domain) only. More importantly, we saw the user playing around with the smartphone instead. Since this user did not seem to take our study and app seriously we decided to sort him out for further considerations.

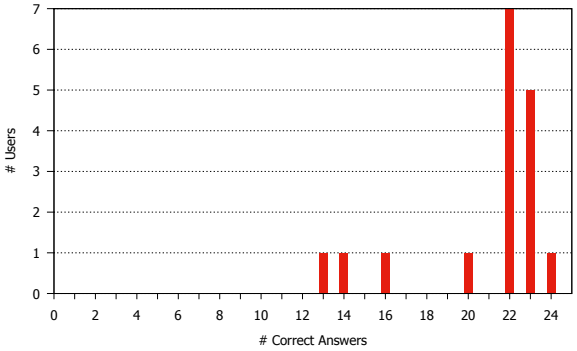
In the following we present the results of our study corresponding to our hypotheses.

Hypothesis 1: Figure 31 shows the results of our study according to hypothesis 1. One can clearly see that the majority of the users identified more URLs correctly after using the app than before. While most participants correctly identified 8 out of 16 (50%) websites before they played the app, almost everyone gave correct answers to at least 22 out of 24 websites afterwards (cf. Figure 31(a) and Figure 31(b)). One could argue that this increase is based on the fact that the examples are mainly the same in the website-survey after, i.e. the reason for their better performance is based on learning effects. Figure 31(c) however shows that the users also performed well for the new URLs. Therefore, we assume the learning effects are negligible. In order to affirm our hypothesis we decided to apply the onesided Wilcoxon signed-rank test [89] with our 16 samples from the website-survey before and the same 16 samples from the website-survey after. Since we consider the learning effects negligible, we do not apply an alternative test against the 24 after URLs. Our null hypothesis is $H_0 : x_1 >= x_2$ and the alternative hypothesis $H_1 : x_1 < x_2$, where x_1 represents the number of URLs which were correctly answered before playing the app and x_2 represents the number of URLs which were correctly identified after playing the app. We computed the positive and negative rank-sums of $W_+ = 141.5$ and $W_- = 11.5$. The test statistic w is the minimum of W_+ and W_-, hence $w = 11.5$. As we chose $\alpha = 5\%$ as significance level and had 17 participants this results in a critical value of 41. As our test value $w = 11.5 < 41$ the null hypothesis can be rejected and thus the alternative H_1 is accepted. Consequently, after playing the app the participants gave more correct answers than before. We are confident that these results cannot entirely be reduced to learning effects. Therefore, we believe that our app helped users to make improved decisions about the legitimacy of URLs.

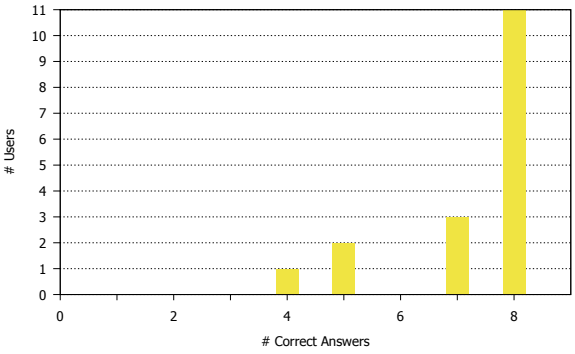
Hypothesis 2: Figure 32 shows how many users marked the URL as their main source of decision. Most of the users already based most of their decisions on the URL before. Occasionally users marked the content or the padlock. However,



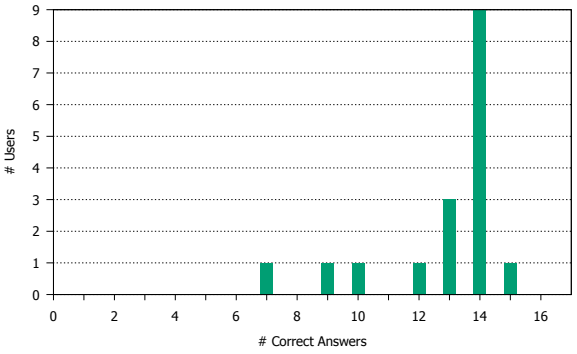
(a) Before



(b) After (Including All URLs)

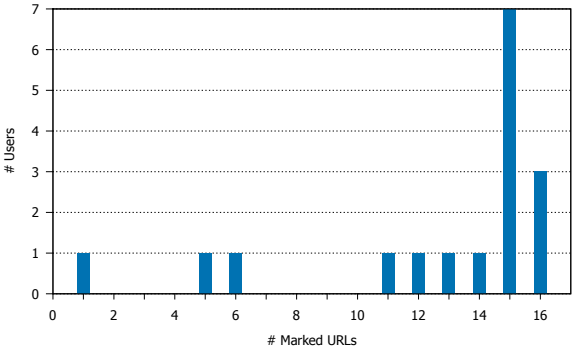


(c) After (New URLs Only)

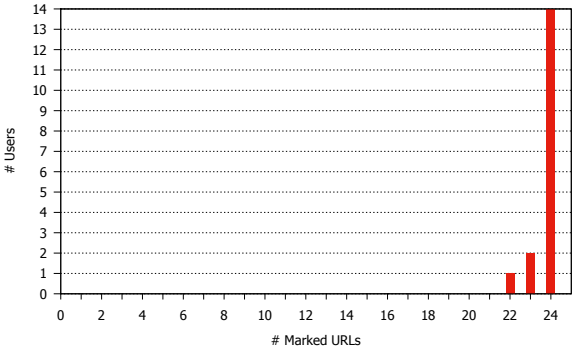


(d) After (Repeated URLs Only)

Figure 31: Correct Answers

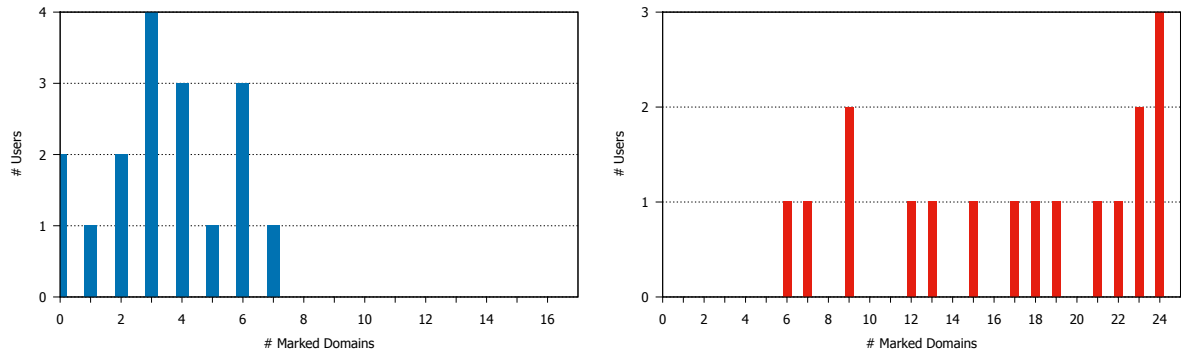


(a) Before



(b) After

Figure 32: URL marked



(a) Before (b) After

Figure 33: Domain marked

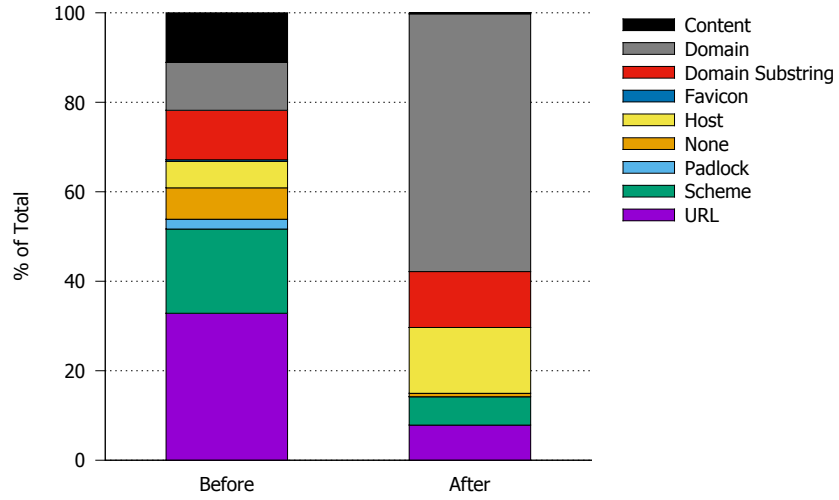


Figure 34: Marked parts of the screenshot before and after

only 3 users (17.65%) always marked the URL. Afterwards, 14 users (82.35%) always based their decision on the URL and only 3 users made one or two mistakes. Therefore, we believe that our app emphasized their belief in basing their decision on the URL. We decided against applying a statistical test to this hypothesis since there is obviously no signficant difference before and after playing the app.

Hypothesis 3: There is a general problem with one question in the websites-surveys. In the before survey we were not able to clearly ask the user to mark the domain when it was the base of his decision because we would have then primed them towards looking at the URL or even at the domain. This would have influenced the results of hypothesis 2. Since we could not formulate this question clearly, a user might have marked the whole URL even if his decision was based only on a small part (for example, the domain) of the URL. Consequently, we were not able to clearly identify what the users' main source of decision was in the before survey. We were aware of this problem beforehand but saw no other option than formulating the question in such an open form. Afterwards, the user knew that they were expected to mark the domain. This can be interpreted as a change of question even if the literal question did not change. Therefore, we cannot apply any statistical tests on this hypothesis. Yet, we want to have a look at the results. None of the users marked the domain in most cases beforehand, in particular, 7 domains out of 16 URLs where marked at most by only one user, cf. Figure 33(a).

Figure 34 shows the distribution of the marked areas before and after playing our app. Obviously, afterwards most of the users marked the domain. However we are not able to compare that to the before values because of the changed

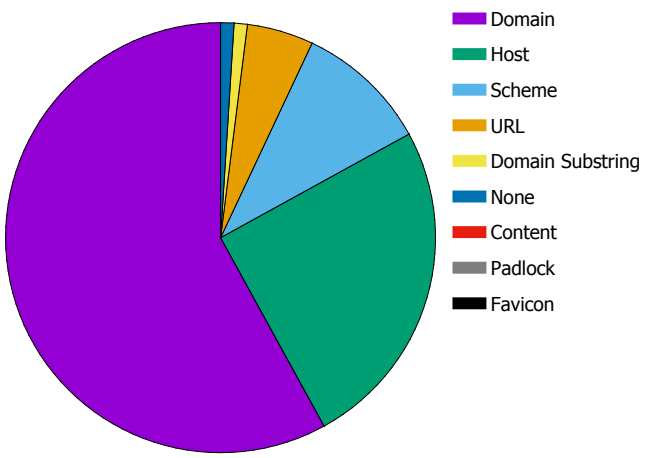


Figure 35: Marked URL parts of legitimate URLs

question. Another interesting observation is that quite a number of participants marked the complete host (instead of the domain) in case of legitimate URLs, cf. Figure 35. One explanation for this might be that we did not ask the user to mark the domain of legitimate URLs except in level 1.

Hypothesis 4: According to the answers that the users gave in the After survey SUS section (section D.3) we calculated a SUS of 83.1. This is above 68 which means that we can consider our app above average usable.

10.5.3 Further Study Outcomes

Besides the results of our hypotheses the study yielded some further interesting outcomes. This section further explores the results we obtained from our survey data and where not part of our hypotheses. Afterwards, we summarize the participants' remarks to our app.

Further Data Exploration

Correct and Reasoned Answers: Hypothesis 1 only refers to giving a correct answer to the question whether a website is a phish or not. Our results show that users did not only give more correct answers after playing the app. In addition to their correct answer they reasoned their answer appriopriately (i.e. marked the domain). In the website-survey before 37.5% of the URLs were answered and reasoned correctly. After playing the app 75% of the URLs were correctly identified and reasoned. Note, that reasoned means by our definition that the domain was marked in addition to giving a correct answer. However, a reasoning must not always rely on the domain itself. As discussed in section 10.5.2, for example, there were numerous participants who often marked the host of legitimate URLs. This is a correct reasoning for their decision, however by our definition it was not considered as such. Also, there were plenty of users who detected a phish and marked the attacked part instead (cf. Figure 29). By our definition this was also not accepted as correct reasoning. Hence, if we had expanded our definition of reasoning even more users would have correctly reasoned their decisions. However, there is the question whether expanding the accepted answers might also result in an increase of the correct answers and markings in the before survey.

False Negatives and Positives: Additionally we considered separately whether the user falsely accepted phishes or rejected legitimate websites. Our outcomes show that before in average the user rejected 4.9 legitimate websites and accepted 2.1 phishing websites. After using the app the user rejected 1.8 legitimate websites and accepted 1.3 phishing websites. One must however note that we increased the users' attention by telling them to look for phishing websites. Additionally usually users tend to behave oversafely in lab situations [90, 91]. Therefore we assume that in this situation, especially before playing the app, users tended to reject URLs in general for safety's sake. This is also reflected by the high

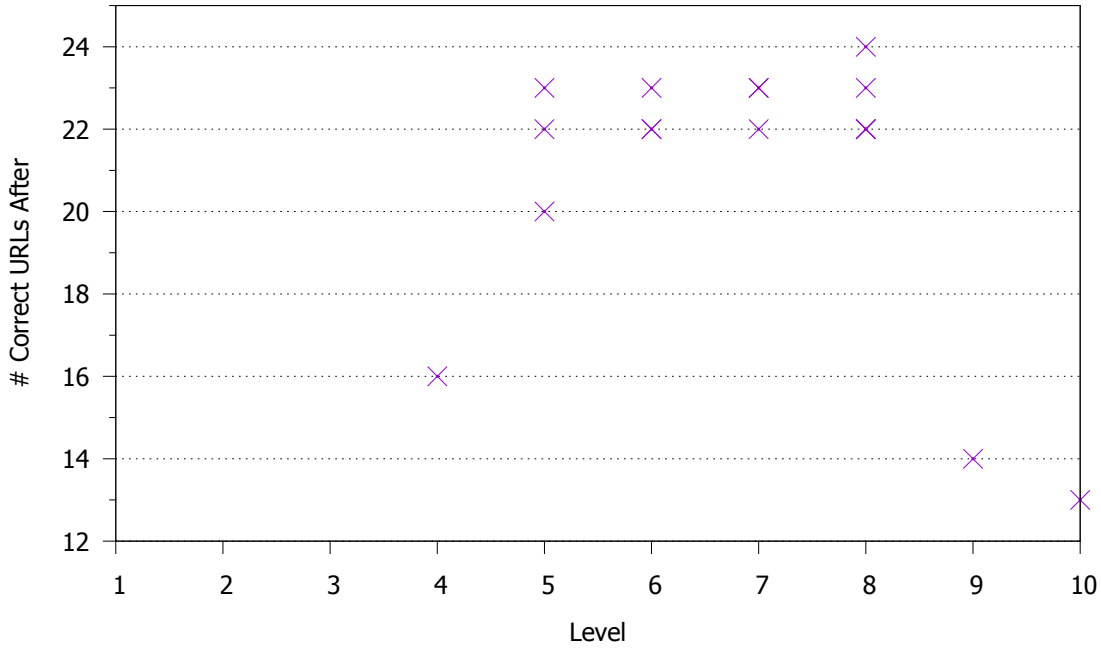


Figure 36: Correct answers related to achieved level

rate of falsely rejected legitimate URLs. In reality however the users contrarily have a interest in entering their personal data otherwise they would have not opened the website. Nevertheless the results show that the users make less mistakes after playing the app and seem to better know why the reject or accept websites (cf. section 10.5.2). In future this should be tested in a more realistic scenario where the users attention is less increased towards looking for phishes.

User Opinions to App: A part of our surveys aspired to understand the users' opinions to our app. Section 3 of our general-survey after (cf. section D.3) contains the statements which the users had to assess with the aid of a 5 point Likert scale. Our worst, but still decent, score referred to whether the user was motivated by the spoofed e-mail to continue playing the app (median of 4) and whether the amount of texts was appropriate (median of 4). All other statements were strongly agreed (median of 5) with in median. The text legibility of our app texts received a median score of 5. Our study participants strongly agreed (median of 5) that our app helped them to identify phishing websites in the future. Finally, the users intuitively understood our three lives scheme per level (median of 5). Thus, the outcomes of the user opinions reveal that our app was very well received by the participants regarding these questions.

Achieved Levels: In average the participants reached level 7, which is higher than we had expected. We assume that some users started to roughly scan our texts for relevant information (for example, mainly looking at the examples) after they understood the importance of the domain. One user even played through the app in 30 minutes. In fact, this user has performed worse by the terms of our definition of correctness. The user had correctly identified 9 (75%) of the URLs before playing the app. Afterwards, he only had a score of 13 (54.17%). The problem was that level 9 deals with the difference of HTTP and HTTPS websites. Pretests had shown that most users would not get beyond level 6. Therefore, we had not considered level 9 in our assessment strategy and regarding its impact on the question. Users were expected to decide whether a website is a phish or not disregarding the usage of HTTPS. The user who has achieved level 9 however was explained the difference of HTTP and HTTPS, additionally, he was asked to reject HTTP sites in general for this level. Hence, this user responded to the website-survey after respectively: the participant generally rejected HTTP sites whether they were phishing or not and thus the user performed worse afterwards by the terms of our definition of correct. All other users performed better after playing the app.

Relation Between Achieved Level and Identified Websites Figure 36 shows the relation between the levels a user achieved and his performance after playing the app. The performance decline of the users that played level 9 or

even 10 is explained in the previous paragraph. These examples are not considered in the following. The Figure shows that playing level 5 already helped users to correctly identify URLs. As we cannot ensure that all users will play our app through, we think it is good that the first levels already provide them the most important input which helps them make more correct decisions on the legitimacy of URLs. Nevertheless, we are confident that the succeeding levels help users detect more advanced attacks and thus are important. Some examples support our opinion: One participant who achieved level 5 fell for an attack that was introduced in level 6 (paypal-sicher.de). Furthermore, 11 participants fell for a phish with scrambled letters (mircosoft.com). These included users who achieved level 6 or higher as well as those who did not achieve this level. In the contrary, those participants who did not fall for this phishing URL at least achieved level 6, i.e. nobody of lower levels recognized this attack. Finally, there are 4 participants who fell for an attack which was introduced in level 8. Three of these participants did not play level 8. Note that all of the services presented by the URLs were known to the users, i.e. it is likely that they fell for the actual attack and did not just assume that the URLs might be legitimate. These aspects indicate that the later levels and training are important to achieve higher expertise. Due to the small sample size, with at most 1-2 examples per attack, it is likely that the above mentioned examples were slightly suppressed in Figure 36. An examination of the relation between the achieved level and the recognized attacks could be done in further research with a larger data set.

HTTPS and Padlock: Our results show that some participants were aware that they should look for either HTTPS or a padlock before playing our app Figure 34. For instance, one participant marked the scheme or the padlock as reason for his decision 11 out of 16 times in the website-survey before. Another participant marked the scheme or the padlock of 8 examples. These participants trusted the padlock resp. HTTPS websites and distrusted HTTP. Consequently, they fell for phishing websites which make use of HTTPS in our survey and are likely to fall for such attacks in reality. Thus, the users who based their decisions on these indicators did not seem to be aware of the fact that the use of HTTPS does not necessarily mean that the website is trustworthy in general. In fact, there are phishing websites using HTTPS (cf. Figure 38). Since we cannot assure that an app user of ours plays until level 9, we believe it is important to introduce the level dealing with HTTPS earlier. This aspect should definitely be considered in future work in our opinion.

User Self-Assessment: Contrary to our expectations, users assessed themselves rather correctly. When asked for their ability of distinguishing legitimate from fraudulent websites at the beginning of the study they rated themselves with 3 on a 5 point Likert scale. Their actual performace in the website-survey before is likewise (56% correctly identified URLs). After using the app they were asked whether the app helped them identify phishing websites in the future. They rated 5 out of 5 and their performance was accordingly good (87% correctly identifies URLs).

Confidence: We asked the users how confident they were about their answers on the website-surveys on a 5 point Likert scale. In median before using the app 3 users stated a confidence of 5. Afterwards, there were 11 users that stated 5 in median. Figure 37 visualizes the overall increase of the users' confidence.

Remarks of Participants

During playing the app, the participants had a slip of paper for notes they wanted to make considering the app. In the following we outline the main results of these slips of paper. Note that we did not ask the users to write down something specific. We merely asked them to write down what they thought, i.e. there might be more participants who agreed with some of these points below but just have not explicitly written it down. In the following we consider the notes and suggestions of all participants.

Scrolling of URL: In addition to deciding whether a URL is a phish or not, the user has to face two more challenges. First, the font size gets increasingly smaller in higher levels, until it eventually is approximately the same size of the Android standard browser. Second, the URL is displayed in a horizontal scrollbar so that the has to scroll the URL to the right in order to view the beginning of it, just like it is the case in browsers. 4 participants found this disturbing and said it hindered them from analyzing the URL reasonably. This supports the importance of the introduction part 2 (access address bar) in the app. The scrolling is present in order to simulate the behavior in the browser and it is important for a user to practice this. We assume that the users would not have noted this in this extent in case they had

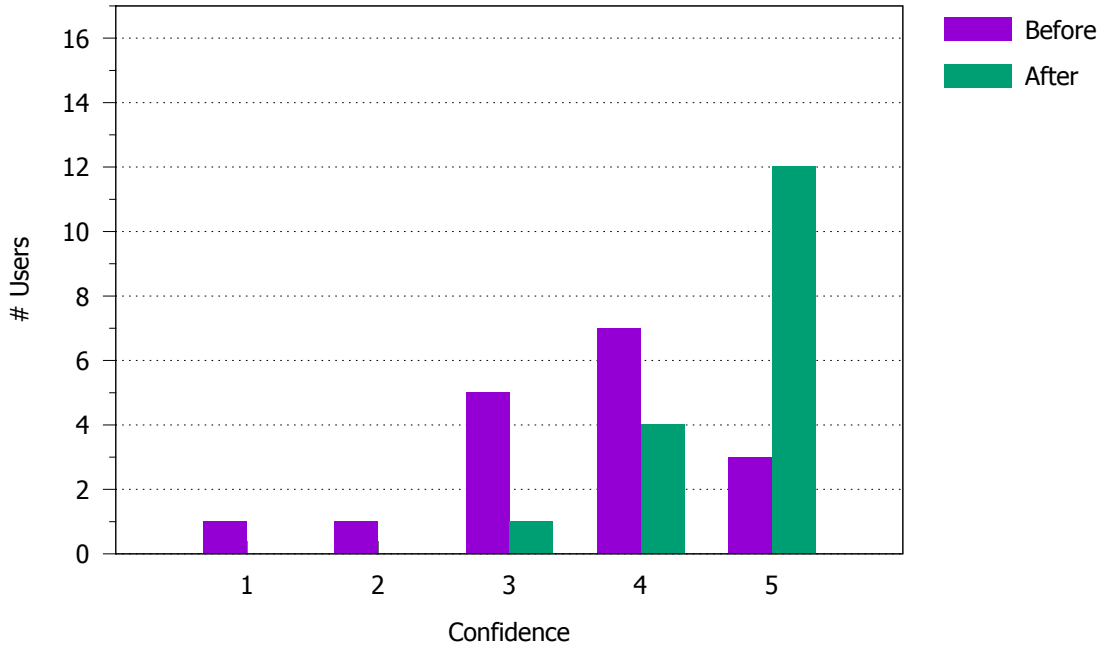


Figure 37: Confidence of the users before and after

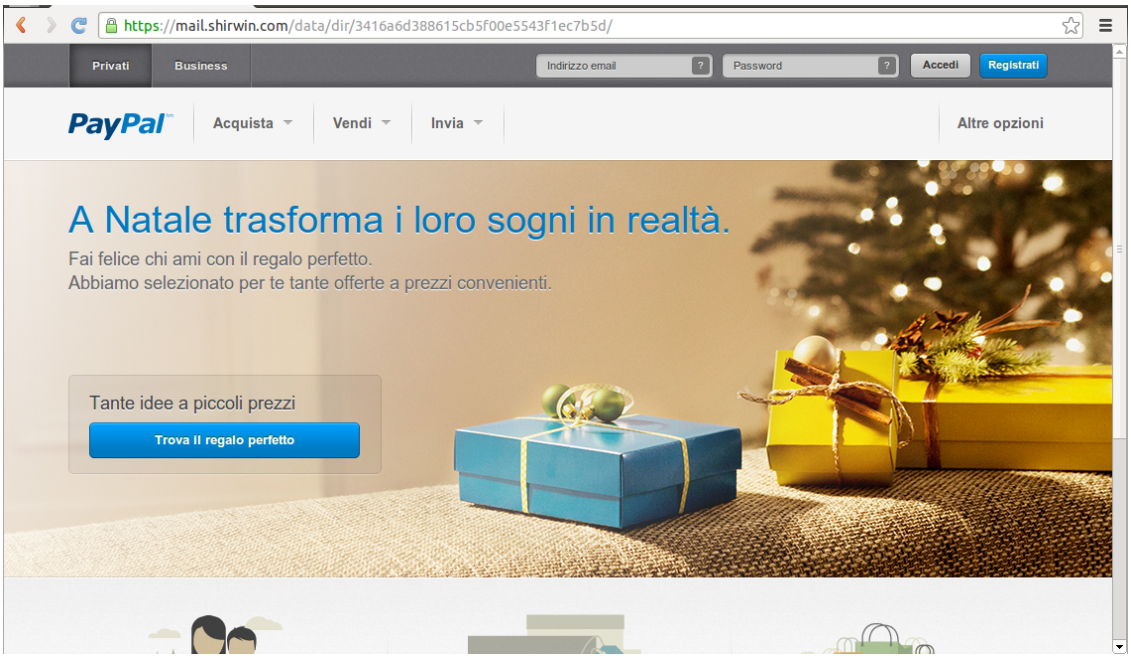


Figure 38: Phishing website using HTTPS [42]

completed introduction part 2, because then they probably would have understood why we do the URL scrolling during the exercises. Yet, we think after a couple of levels the users should have understood that they have to scroll the URL, in the game as well as in the browser, so one might consider to reduce or eliminate it after some time.

Unknown Services: We have mentioned the problem of unknown services in section 7.4.2. As we were afraid there are in fact services which are not familiar to several users. Several participants mentioned this problem. Even if we tried to make use of the most popular services with the aid of Alexa's [92] ranking we cannot assure that all used URLs are known by all users. One idea to approach this challenge might be to provide an question mark button in addition to the check mark (no phish) and cross mark (phish) buttons. When a player clicks on this button, he can be told whether the given URL is a phish or not and why. From this action the user would neither profit nor would he lose any points or lives. Yet, we do not think that this is a major issue, since the users got at least until level 4 and most of them achieved even higher levels. We are confident that the app in its current state is already implicitly able to teach the users about the legitimacy of unknown services. After facing unfamiliar URLs and making or not making mistakes they will eventually learn whether to trust a service or not.

Question to Data Entry: Some participants noted that the formulation of our website-survey question "Would you enter your sensitive data into this website?" was ambiguous. Thus, there might have been participants who selected "no" even if they did not think it was a phishing website, but they would generally not enter their data into this specific website. Originally, the website-surveys before and after asked the participants whether they thought a given website screenshot was a phishing website or not. After our test iteration of our study, however, we decided to add some context to the question and had to make this trade-off with respect to the new question's ambiguity. As we told the user that this study was particularly about phishing and that their task was to detect phishing websites in the website-surveys before and after, we believed that the ambiguity of this question would be negligible.

Explanations and Comprehensibility: 4 participants stated on their slips of paper that they found the explanations of the app very good and easy to understand. 1 of these 4 participants, however, added that there is partially much text to read. Another participant (not under those 4) noted that there is too much and long text in general.

Button Positioning: The positioning of our app buttons during the game are as follows: The left bottom corner has a check mark which represents that the user thinks the displayed URL is not a phish. The right bottom corner has a cross mark which means that the user thinks the displayed URL is a phish. After clicking on either of these buttons in the write bottom corner another button appears (where the cross mark usually is) which either is the continue or the verify button (depending on whether the user has to select the Who-Section or not). Some participants indicated that the positioning of the buttons in the right bottom corner are suboptimal. The problem is that accidentally double clicking, for example, the continue button in the right corner results in rejecting the next URL even if the user might not have intended to. Even if not many participants explicitly criticized this aspect we believe that this is a justified point. In fact, the positioning of the two buttons continue and verify should be different from the one of the cross mark. This is an aspect which should be targeted in future work.

Repetition: Repetition is an important element of our app. In every level introduction we briefly repeat the so far learned parts of a URL (with a graphic) and the different attacks the user has seen until this point. We also make use of repetitions during the exercise rounds, every level contains at least one exercise from the previous level. Some of our participants explicitly indicated that our repetitions made them feel more confident and safer.

External Links: In the main menu of our app we have a button "More About Phishing" which leads to a list of external links to various websites about phishing. Some of these websites are in English. Some participants indicated that they did not like it to be led to an English website and would have preferred to be forwarded to a German one. This reveals that we cannot expect our audience to have knowledge of the English language. Therefore, only German websites should be linked in the future. Another idea to approach this might be to provide in-app additional information. That is, instead of linking to external websites, the app itself could provide additional categorized information in German. This would solve the problem with the language of websites and at the same time the additional information would fit to our app layout and design.

Amount of Examples: Our app starts with a small sample of URLs users have to decide on. In every level the sample size increases as the number of possible attacks increases. Only 2 participants found that our sample size was too large. This might have been the result of the fact that the users had to play the game for half an hour at a time. We believe that the number of examples are reasonable, assumed that a user does finish the app at a stroke.

Further Suggestions: In their notes some users made several suggestions which we found interesting. These suggestions include, for example, more text highlighting of new teaching contents or the suitability of our app to be applied in schools. In section 11.3 we elaborate on aspects for further research in more detail.

10.6 Limitations

We decided to conduct a study which compares the users' performance before and after playing our educational app. Our study design has some limitations we were not able to address for several reasons that we are going to discuss subsequently.

Behavior Change: In our study the participants were not in their usual environment. Therefore, they likely behaved differently during our study. An alternative approach would have been to distribute the app to several participants and ask them to play it remotely. However, this has two major downsides: First, the user would have been remote and thus we would have less control. Second, testing the before and after app skills would have been difficult to realize in order to ensure a homogenous process among all participants.

Increased Attention: At the beginning of the study the participants were told that the study dealt with phishing. Additionally, for the website-survey before and after they were explicitly asked to indicate whether the websites were phishing or not. That is to say, the user automatically increased his attention towards answering these kinds of questions. Designing an in situ study, where the participant would have been in their usual environment and would have not known about their participation, was not considered because such a design is ethically and legally questionable.

Knowledge Retention: Our study design focuses on the present. Given certain time boundaries, it was not possible to study the long-term influences of our app by conducting the after app scenario repeatedly. Consequently, knowledge retention is an aspect which is not considered by our study.

Bias: For the recruitment we endeavored to ensure that our participants are not close friends of ours. We rather seeked for friends of friends or even completely unknown persons (cf. section 10.1). Certainly, the presence of a minor bias cannot be totally excluded.

Despite the limitations of our study we are confident that we got a good insight into the effectiveness of our app.

10.7 Discussion

Our hypotheses stated that our app can increase three major skills of the user. First, we wanted to give the user the ability to detect phishing URLs. This goal can be considered achieved as we could show that the increase is significant. Even though there might be some learning effect we are confident that this increase is not mainly attributable to that. The second and third hypotheses focused on the reasoning behind the user's decision. We wanted to show that the user is aware of the fact that the content is no source of evidence against a phishing attack. Our results suggest that most of the users already feel that the URL is important beforehand but some additionally consider the content. Thus, the change in user response was not high enough to measure our hypothesis 2. The third hypothesis said that the users understand the structure of URLs better after playing our app. As we discussed above, we had concerns about the design of the question that was intended to test this hypothesis. The question has to be regarded as changed after playing the app. Due to this, we could not consider the before-markings and could not argue on any findings about this hypothesis.

In addition to testing the hypotheses we got overall positive feedback from the users. Most of them had the feeling they learned something from the app. Some participants even contacted us asking about the release date of the app because they wanted to give it to their relatives.

Yet, there are still some improvements that should be considered when someone develops a next version of the app. First of all, we think that the part talking about HTTP and HTTPS should be moved to an earlier level. We saw many users that marked the scheme or the padlock in the URLs in the website-survey before. This seems to be more important for the user than the URL itself because we had several users who fell for a phish and marked the scheme or padlock as reasoning. As we cannot assume that users finish our app within one day, or even finish it at all, we think that it is important to clear that misunderstanding earlier. The second improvement that a following developer should include is to restructure the app texts in such a way that the user can clearly identify repeating and new parts. We think this aspect is not as important in real life compared to study situations because the app is not designed to be played a long time in a row. This would increase the importance of the repetitions and make such a separation less important but this can be improved. Last, it might be a good improvement to modify the app behavior depending on the user skill and performance. This might prevent the user from getting bored. This includes, for instance, vary feedback texts and icons depending on the user's performance as well as the degree of difficulty. Another example is that the app could skip the proof part (identify Who-Section after detection of a phish) in case there is an indication that the user understood how to do it. A simple form of that is already implemented. The proof is shown up to a predefined level. Yet, we think it is more reasonable to base the skipping and other possible extensions on the user performance.

To conclude our findings despite some possibilities for improvement we can say that the app helped most of the users detect phishing URLs. This means we overall achieved the goal of the app.

11 Conclusion, Lessons Learned and Future Work

This chapter provides a short summary of what we achieved within the scope of this thesis and some further concluding remarks. We also present a short list of recommendations regarding the design of security education games based on the lessons we have learned. Finally, we provide an outlook on future work.

11.1 Conclusion

The objectives of this thesis were twofold. First, we aimed at increasing users' security awareness hoping to provoke a change in their security related behavior. Second, we focused on the education of users with regard to the detection of phishing URLs. Our app is supposed train the user to achieve the required capability of correctly parsing URLs and thus identifying phishing websites. This new knowledge will eventually help them defend themselves against the steadily increasing phishing attempts.

To achieve these goals we developed an anti-phishing education quiz based game. Our app targets the increase of security awareness by actively let the user spoof an e-mail and by exemplifying him that a link does not necessarily lead to the target that it displays. By letting the users practically experience this, we hoped to increase the intensity of their learning experience (cf. Principle of Intensity in section 8.6.1) resulting in a better and higher learning performance and motivation. In fact, in median the users rated 4 out of 5 (strongly agree) that this part of the app motivated them to continue. After motivating the user with the practical example and increasing his security awareness the actual game starts. The game itself consists of levels with introductory parts followed by practical exercises the user has to solve in order to show he has understood the learning content. Initially, in introduction 2 (access address bar and view complete URL) and level 1 (URL basics and domain identification), basic knowledge is covered which is required for the succeeding levels and especially for the detection of phishing URLs on the smartphone in general. In particular, introduction 2 might be not challenging enough for some users as they might be already well-skilled regarding smartphone functionalities. Yet, this introduction and exercise is indispensable as there can be users who do not know how to approach this. In levels 2-9 the user is introduced to various attacks a phisher might apply. These attacks get increasingly sophisticated and harder to detect with higher levels. Finally, in level 10 the user gets further final remarks, such as the discussion about legitimate URLs which may appear fraudulent but in fact are not, or input to extended validation certificates and a link for further information.

We generally aimed at using introductory texts that are simple and easy to comprehend. We evaluated this by directly asking our participants in one of the study surveys (cf. section 10.5.3) and by computing the legibility index of our texts (cf. section 9.3). Both results confirmed the achievement of our goal in this regard: in median the users rated 5 out of 5 that our texts are easy to understand. Furthermore, our final legibility index of 62 is considered as reasonably comprehensive for teenagers [84]. The study outcomes suggest that there is a positive effect resulting from our app. Our participants clearly gave more correct answers, to the question whether a given website is a phish or not, after playing the app compared to before. Before playing the app most users identified 8 (50%) of the 16 websites correctly. After playing the app the majority of the participants gave correct answers to at least 22 (91.67%) of the 24 websites. We assume the learning effects are negligible as the distribution of the correctly answered new URLs is almost identical to the old one (cf. Figure 31(c) and Figure 31(d)). The results of our second hypothesis exposed that the users already knew it was important to look at the URL before playing the app. Yet, they obviously did not know where exactly too look at as their result in correct identifcations show. Even if there were many participants who looked at the URL already before playing the app there is a significant difference in the following aspect: Before playing the app only 3 (17.65%) users always marked the URL. In contrast to that, after playing the app most, i.e. 14 of 16 users (82.35%), always marked the URL. Evidently, our app was able justify and further emphasize their belief in basing their decision on the URL rather than the content or anything else. The measurement of our third hypothesis was questionable. The participants were asked to mark the reason for their decision whether a given website was a phishing attempt or not, before and after playing the app. Here, the problem is that we could not formulate the question without implicitly pointing them towards marking (parts of) URLs instead of any other indicators of the browser or website itself after playing the app (because the app asked them to mark the domain). That is, before using the app the users might have meant the domain, but just did not clearly mark it and marked the entire URL instead, because they did not know what exactly they were expected to mark.

After playing the app they knew what they were expected to mark and thus might have marked more precisely. Still, we analyzed our results on this question and found out that more people base their decision on the domain after playing the app.

Our study outcomes support that our app helped users make better decisions on the legitimacy of URLs. A further analysis of long-term effects would be valuable. The question to ask here is will this app actually help users change their behavior in the Internet persistently and make them look at the URL even if it is only occasionally. This is an aspect, which we were not able to address within the scope of this work. Furthermore, our final conducted user study cannot show how the users, for example, retain the lessons learned from our app. Such considerations remain open for future work. All in all, we implemented a valuable complementary approach to technical solutions, an approach that encourages the user to protect himself by using our app that educates him on this topic.

11.2 Lessons Learned

Technical solutions are not 100% accurate at detecting phishing attacks. The education and training of users offers a complementary approach to these systems. Based on our gained experience, we present a brief summary of our lessons learned from this work. These lessons might be helpful for further research in the area of security education.

Principles of Learning: Since education games do not primarily aim at entertaining the users, but simultanously at educating him, it is important to take the principles of learning into account. These principles state under which conditions learning performance is increased (cf. section 8.6.1). We consider it especially important to rely on the principle of exercise, which states that training, repetition and feedback is crucial for good learning performance.

Game Techniques: If education is supposed to follow with the aid of a game it is relevant to regard essential game techniques (cf. section 8.6.2). In fact, game techniques are closely connected to learning principles. They provide in-depth elaborations on how basic learning principles are achieved with games.

Simple and Short Text: Education implies that some sort of text is present in some way. The users to be educated may come from different fields. While some users might be more skilled and might be able to handle complex texts on security-related topics others would probably get discouraged by such. Skilled users are likely capable of acquiring knowledge on security topics without problems. Security education should mainly address those users who are overwhelmed by such texts and information. For these users it is important to provide simple texts which are easy to follow and not too long. The longer texts are the more likely it is that the users will skip text parts, which might be important, or even stop reading it.

Precise Phrasing: The texts should be formulated precisely. If a text is not precise this might lead to misinterpretations and thus to mistakes. One should take care that there is as less room left for misinterpretation as possible.

General Validity: There is a range of potential learning content which might be important to communicate to the users. Yet, there is the problem of general validity. It is important to consider that, for example, aspects that apply to system A, for example an Android device, do not apply to system B, for example another version of the same Android device. Therefore, in some cases it might not be easy to transfer knowledge about A to B (such as the browser functionality). For this reason it is relevant to consider whether one wants to educate the users about aspects which are generally valid among several systems or whether the education focuses on specific systems which ultimately would result in restricting the target audience to those who use that specific system.

11.3 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 address and realize due to time and resource limitations.

11.3.1 Conduct Further Studies

Comparative Study: A comparative study, as the authors of Anti-Phishing Phil [22] did, might be interesting. They conducted a study with three different conditions, a group that consulted general tutorials from the Internet, a group who learned from tutorials based on Anti-Phishing Phil and another group who played Anti-Phishing Phil itself. An interesting comparison would be our app with Anti-Phishing Phil or any other anti-phishing app and general tutorials. For example, the impact of the various approaches on the users' performance could be compared. Additionally, one could test whether some approaches are better received by users than others.

Study on Retention: For time reasons knowledge retention is an aspect we could not address in our study. Yet, we think it is important to consider this in future work. The question to ask here is how well users retain the knowledge they obtain from our app compared to other sources, for instance.

In-App Statistics: If the app is published on google play and gains a large user group it might be interesting to use that group for an in-app study. This means the app could be changed in such a way that it collects statistical data from the playing users and reports them back to the working group. Based on this data further exploration could be done. When implementing such a logging function, one should consider the ethical and legal implications that are posed. Such a functionality can also influence the users' acceptance of the app. Furthermore, such a large collection of user data might be misused by a potential attacker. Therefore, technical security considerations would be of relevance as well.

11.3.2 Extend Teaching Content of App

Malicious Downloads: With our app we did not target the possibility of downloading malicious software when a user clicks on a link. However, we think this is an aspect which should be targeted in future work since malicious software can also cause harm. For example, the user could be told at some point that he should never open downloaded files he did not intend to download. Instead he should immediately delete them.

Certificate Validation: We do not address the validation of certificates with our app. We also do not tell the user, for example, that he should not do online banking or online payments in general in case a certificate is broken. Such general suggestions might also be considered in future work.

Data Economy: Another interesting aspect we did not cover in our app is data economy. We tell the user to type in their data only into websites they are sure about their legitimacy. However, we do not tell the user to think about the specific data they are asked to enter. Users should re-think whether the required information is actually needed. This should also be trained by for example asking the user "A lottery site is asking for your data. Which data would you provide?". As this approach would require a complete different UI this type of learning content remains for future work.

Consequences: Another idea is to to display the consequences for falling for a specific phishing URL (matching a certain website category). We believe that this kind of information is relevant for the user as it illustrates him on which websites he should especially take care, for example, on banking websites. Therefore, this should be considered in future versions.

Top-Level Domain Attacks: It might be reasonable to explicitly tell the user that he should not only look whether the second-level domain is exactly as he expects but also the top-level domain. The app only implicitly states to look at the top- and second-level domain together. We recognized that users might misinterpret this (problem of precision). Therefore, this addition should be realized for future versions.

Introduce HTTPS Earlier In section 10.5.3 we showed that it is important to introduce the teaching content related to HTTPS to an earlier level in order to assure that users do not fall for phishes using HTTPS.

Text Improvements: After conducting a guerilla user study on our app texts the contents of levels 9 and 10 were changed. These changes have not been thoroughly tested by users yet. This needs to be done and the texts should be modified accordingly.

Add context: Currently, the app does not display any context regarding the process of how the user reached the URL or regarding what is displayed on the website. We believe that the context of a situation should have an impact on a user's decision of whether to enter personal data or not. To address this, some kind of context could be added.

11.3.3 Improve Game Experience of App

Increase Immersion: Immersion is an important game element (cf. section 8.6.2). We believe our app has space for more immersion beyond our analogy which considers a website as a user's communication partner. For example, an appealing story could be added to our quiz game in order to further mesmerize the user. One example story could be the following: the player is hired by a renowned company and his job is to find phishing websites and put them on a blacklist so that employees of that company do not fall for them. If the user does a bad job he suffers reputational damage, wage reductions or might even lose his job. If he does a good job he can climb the career ladder.

Increase Effect: In section 8.6.1 we have introduced the Principle of Effect, and more specifically, the law of positive feelings. We believe the user's positive feelings can be increased by providing more varying feedback, instead of saying the same sentence for the same outcomes. For example, the praises and compliments when a user does well could vary depending on the degree of difficulty. Also, the final screens for finishing a level can vary respectively depending on the achieved score in order to address higher and better positive feelings.

Performance Dependent App Behavior: More dynamic behavior could be added in future versions of the app. For example, the part where the user has to show the domain in case he found a phish might get tedious after some time. To approach this problem the app could stop asking for the domain after the user identified the domain correctly n times in a row, for example. After this point the app could occasionally ask the user to identify the domain and depending on his performance re-introduce it.

Text Highlighting Some users suggested to visually separate new learning content from repetition so that skimming over the information part becomes easier. This is partially done already. Yet, the emphasis and separation of new and relevant learning content in the lesson parts could be improved in future work.

Improved Button Positioning In paragraph 10.5.3 we discussed that the same positioning of the "verify", "continue" and "cross mark" buttons are suboptimal for the following reason: Clicking on, for example, "continue" results in a new challenge view with a new URL. Therefore, accidentally double clicking on the continue button can lead to clicking on the cross mark, and ultimately to the rejection of the URL (before even looking at it). Therefore, the positioning of the two buttons continue and verify should be different from the one of the cross mark. This is an aspect which should be targeted in future work.

11.3.4 Miscellaneous

Combination of Embedded Training and Education Application: In section 3 we argued that exploiting the teachable moment might motivate a user to do something about his lack of knowledge regarding phishing and possibly result in better retention. Yet, a drawback of embedded training is that its landing pages should not provide too detailed and extensive information on the topic since users may get discouraged and leave the page. Providing detailed and extensive information can be addressed by a game playfully. Therefore, an idea is to combine embedded learning with an educational game. Here, if a user fell for a simulated phishing attack he would be forwarded to the landing page. This page could provide the user with the most important information and a link to an educational app, for example ours, where he can optionally get more detailed information. With the game extensive knowledge can be obtained step by step by playing the it. However, there remains the problem of the legal issues raised by sending out simulated phishing e-mails on behalf of a well-known vendor.

Integration of App into School Education Further research could address the integration of our app into school education. People might not want to learn about phishing by their own choice, especially pupils would probably not think

about that. However, if computer security is a part of the education plan and if pupils have to learn something about phishing by playing the app, for example, a far larger audience could be addressed and educated on this topic.

More Appealing Outer Appearance Even though we considered the user interface design and some icons to enhance the outer appearance of our app, we did not focus on design aspects. Yet, we believe a more vivid outer appearance might help us draw more potential users.

A E-Mail Template of the Awareness Part

```
<html>
  <head>
    <title>Anti Phishing Education</title>
  </head>
  <body>
    <p>Dies ist eine automatisch generierte E-Mail im Rahmen einer Anti-Phishing
       Education App. Falls diese nicht angefordert wurde, bitte ignorieren.</p>
    <p>Ansonsten geht es hier weiter:</p>
    <p>Wie du im Absender siehst, hast du dir gerade selbst eine E-Mail mit gefä
       lschtem Absender geschickt. Hier ist außerdem dein Freitext:</p>
    <p>{$usermessage}</p>
    <p>Für einen Angreifer ist es ebenso einfach automatisierte E-Mails mit gefä
       lschtem Absender und Inhalt zu verschicken. Meist enthalten diese einen Link zu
        einer Webseite, genau wie diese E-Mail.</p>
    <p>Um mit der App fortzufahren, klicke auf den folgenden Link.</p>
    <p><a href="http://pages.no-phish.de/maillink.php">http://www.google.com</a></p>
    <p>Viele Grüße,</p>
    <p>Dein NoPhish Team</p>
  </body>
</html>
```

B URL Generation Process

When playing the app (level 2-9) the user has to categorize a given URL as a phish or valid URL. We decided against a fixed set of examples for the URLs because depending on the set size it might happen that a user keeps being confronted with the same URLs. We believe it is essential for the user to be faced with as many different URL examples as possible. Therefore, we decided to generate the URLs rather than composing a fixed list. Next, we lay out the URL generation process and cover further interesting aspects of the URL generation in the subsequent sections.

B.1 Derive Phishing URLs from Legitimate Example URLs

To present attacked URLs to the user we found it most realistic to take valid URLs and apply the covered attacks to them. For this purpose, we needed a set of legitimate URLs. To build this set we used Alexa [92] to select various domains from the top 100 website vendors of Germany. Then, we visited each of these websites, navigated through them and picked about 3-6 URLs for each domain we had previously selected. We strived to balance the number of short and long URLs. Given a list of valid URLs an attack can be applied whenever required. In the following we discuss how this is accomplished in our implementation.

Generate a List of Attacks for Each Level: When starting a new level we generate a list of attacks with which the user needs to be confronted.

Select a Valid URL: Whenever a new URL is to be shown to the user we first randomly select a valid URL from the aforementioned set.

Modify Valid URLs with a Generator: Then we apply a generator to the URL that does not invalidate the URL but modifies it (cf. section B.3).

Apply an Attack: After that we select a random attack from the previously built list and apply it to the selected valid URL.

Repeat in Case Attack was not Possible: In some cases applying a specific attack to a given URL is not possible. For example, in homograph attacks the replacement of an “i” with another letter in a URL which does not contain an “i” will fail. In these situations we have to retry.

B.2 Number of Phishes and Repetitions per Level

The types of spoofed URLs the user is faced with depends on the level. Each level introduces one ore more attacks. The introduced attacks of each level are layed out in section 8.4. In general, the URLs of each level n are distributed as follows: Repetitions are also included into the list of attacks to be applied which is created upon start of each level. The

Total number of URLs	u	$6+2*n$	Starting with 6 URLs each level has 2 more URLS.
Number of phishes	p	$u/2$	Half of the URLs are phishes.
Number of repetitions	r	$\lfloor p/2 \rfloor$	Half of the phishes are repetitions.

Table 3: Distribution of URLs per level

list of repetitions is filled up as follows: every level has exact one attack repetetion for each previous level. The rest of the repetitions is filled up randomly. This way, we assure that at least one example of each previous level is represented by the attack repetitions. All remaining phishes are new attacks. There are two main exception to these rules:

Level 1: In level 1 the user is only confronted with valid URLs and has to select the domain. To prevent the user from getting bored we only present 5 URLs in this level. None of them is a phish.

Level 1+2: The first level that contains repetitions is level 3 because level 2 introduces the very first spoofing attack. Consequently, level 1 and level 2 do not have repetitions.

B.3 Modify Legitimate URLs with a Generator

We were unsure whether we had collected sufficient valid URLs. For this reasons, we prepared a way to automatically modify the URLs in such a way that they remained valid URLs. Some ideas were to add subdomains or path strings to the URL. Queries or fragments would also be possible. Later we found out that it was currently not required to implement such generators since our set contained enough URL examples. Yet, if we should realize in future that these URLs are not enough we have this scheme in place.

B.4 Re-Apply an Attack in Case of Wrong User Answer

After generating a valid URL we choose a random attack from the previously built set of attacks and apply it to the URL. We also store which attack we currently apply. This is important in case the user fails to give a correct answer to the current URL. In this situation we will simply readd this attack to the set of attacks. This way, we assure that the attack, which the user failed to identify, is repeated later in this level.

C Questionnaire of Study for Input

Fragebogen zu Phishing im Internet

Im Rahmen unserer Studie möchten wir das Bewusstsein über Gefahren im Internet erforschen. Wir würden uns freuen, wenn Sie sich die Zeit nehmen könnten, uns ein paar Fragen zu beantworten. Die Daten werden natürlich anonymisiert gespeichert, sodass kein Rückschluss auf Ihre Person erfolgen kann.

1. Generelles

Zuerst ein paar generelle Fragen zu Ihrer Person.

1.1. Ihr Alter.....	_____			
1.2. Ihr Geschlecht	☐Männlich	☐Weiblich	☐Anderes	
1.3. Beruflicher Abschluss				
☐Lehre	☐Meisterprüfung	☐Hochschulabschluss	☐Keiner	
1.4. In welchem Bereich arbeiten/studieren Sie zurzeit?	_____			

2. Internetnutzung

Es folgen einige Fragen zu Ihren Erfahrungen im Internet.

2.1. Wie häufig sind Sie online?						
☐Ständig	☐Mehrmals täglich	☐Täglich	☐Mehrmals wöchentlich	☐Seltener		
2.2. Welche Anwendungen des Internets verwenden Sie?						
☐E-Mail	☐Browser	☐Banking	☐Medien (Audio, Video)	☐Spiele	☐Soz. Netze	☐_____
2.3. Verwenden Sie ein Smartphone?						
☐Nein	☐Ja, Android	☐Ja, Apple	☐Ja, _____			
2.4. Wenn ja, welche Anwendungen verwenden Sie auf Ihrem Smartphone?						
☐E-Mail	☐Browser	☐Banking	☐Medien (Audio, Video)	☐Spiele	☐Soz. Netze	☐_____
2.5. Wie viele Werbemails bekommen Sie pro Woche ca.?						
☐< 10	☐10-20	☐20-50	☐50-100	☐> 100		
2.6. Wie viele E-Mails, die Sie nach persönlichen Daten fragen, bekommen Sie pro Woche ca.?						
☐< 10	☐10-20	☐20-50	☐50-100	☐> 100		
2.7. Ich informiere mich über Gefahren im Internet und wie man sich davor schützen kann.						
☐Nein	☐Ja, selten	☐Ja, gelegentlich	☐Ja, regelmäßig			

3. Einschätzungen

Im Folgenden sollen Sie entscheiden wie sehr Sie den entsprechenden Aussagen zustimmen.

Bitte bewerten Sie zwischen 1: „Trifft voll zu“ und 5: „Trifft überhaupt nicht zu“	1 trifft zu _ 5 trifft nicht zu
3.1. Ich kenne mich gut genug aus, um den Gefahren im Internet aus dem Weg zu gehen.	1 □ 2 □ 3 □ 4 □ 5 □
3.2. Es fällt mir leicht legitime von gefälschten E-Mails zu unterscheiden.	1 □ 2 □ 3 □ 4 □ 5 □
3.3. Sicherheit im Internet bezieht sich ausschließlich auf Finanzanwendungen.	1 □ 2 □ 3 □ 4 □ 5 □
3.4. Meine Daten gebe ich im Internet nur an Anbieter weiter, die ich gut kenne.	1 □ 2 □ 3 □ 4 □ 5 □
3.5. Mir persönlich ist es egal, was mit meinen Daten im Internet geschieht.	1 □ 2 □ 3 □ 4 □ 5 □
3.6. Für den Schutz vor Gefahren im Internet ist jeder selbst verantwortlich.	1 □ 2 □ 3 □ 4 □ 5 □
3.7. Ich vertraue E-Mails, die von mir bekannten Personen kommen.	1 □ 2 □ 3 □ 4 □ 5 □

4. Phishing

Die folgenden Fragen beziehen sich auf einen Angriff, der allgemein als „Phishing“ bezeichnet wird.
Dabei wird versucht dem Nutzer Daten durch gefälschte E-Mails oder Webseiten zu entlocken.

4.1. Folgende Dienste sind durch Phishing gefährdet.

☐E-Mail	☐Browser	☐Banking	☐Medien (Audio, Video)	☐Spiele	☐Soz. Netze	☐_____

4.2. Folgende Daten sind durch Phishing gefährdet.

☐PIN/TAN	☐ Kreditkartendaten	☐ Zugangsdaten	☐Pers. Daten (z.B. Geburtsdatum, Adresse)

5. Anti-Phishing Anwendung

Ein Teil der weiteren Studie soll die Entwicklung einer Smartphone Anwendung sein. Diese hat das Ziel den Benutzer über die Gefahren von und Abwehrmechanismen gegen Phishing-Angriffe zu informieren. Zur Vorbereitung dieser Entwicklung interessieren wir uns für Ihre Vorstellungen zu einer solchen App.

Bitte bewerten Sie zwischen 1: „Trifft voll zu“ und 5: „Trifft überhaupt nicht zu“	1 trifft zu _ 5 trifft nicht zu
5.1. Passend zum Begriff Phishing fände ich ein Spiel mit einem Fisch lustig.	1 □ 2 □ 3 □ 4 □ 5 □
5.2. Um Wissen zu vermitteln ist ein Textbasiertes Programm am sinnvollsten.	1 □ 2 □ 3 □ 4 □ 5 □
5.3. Mit Frage-Antwort Spielen macht mir Lernen am meisten Spaß.	1 □ 2 □ 3 □ 4 □ 5 □
5.4. Zum Auflockern von Wissensvermittlung sind Comics ein gutes Mittel.	1 □ 2 □ 3 □ 4 □ 5 □
5.5. Zum Verfestigen des Gelernten sind Übungen unerlässlich.	1 □ 2 □ 3 □ 4 □ 5 □
5.6. Mich begeistern häufig Lernspiele.	1 □ 2 □ 3 □ 4 □ 5 □
5.7. Wichtig ist, dass mich ein Lernprogramm immer wieder überrascht.	1 □ 2 □ 3 □ 4 □ 5 □
5.8. Bei einer Anti-Phishing-App müsste ich für mich sofort feststellen können, dass es mir etwas bringt.	1 □ 2 □ 3 □ 4 □ 5 □
5.9. Gut fände ich eine Trennung zwischen dem Lern-Modus, dem Übungs-Modus und dem Test-Modus.	1 □ 2 □ 3 □ 4 □ 5 □

5.10. Folgende Idee/Anmerkung/Vorstellung habe ich für Ihre App.

5.11. Was müsste das Spiel bieten damit Sie es verwenden würden?

✂----------

6. Weiterer Studienverlauf

Möchten Sie über den weiteren Verlauf der Studie informiert werden? Die Antworten in diesem Abschnitt werden getrennt von den obigen verarbeitet und gespeichert.

6.1. □ Ich möchte über den weiteren Verlauf der Studie informiert werden.

6.2. □ Ich bin bereit eine im Rahmen der Studie entwickelte Smartphone-App zu testen.

6.3. E-Mail-Adresse _____

7. Dank

Vielen Dank für ihre Teilnahme an unserer Umfrage.

D Final Study

D.1 Participant Recruitment

Sehr geehrte/r ....,

wir, Clemens Bergmann und Gamze Canova, sind Studenten des Fachbereichs Informatik an der TU Darmstadt und arbeiten zur Zeit unserer Masterthesis zum Thema Internetsicherheit.

Nun sind wir an dem Punkt angekommen, an dem wir eine Benutzerstudie (6.1.-11.1.2014) durchführen müssen, für die wir Teilnehmer suchen. Wir würden uns sehr freuen, wenn Sie uns hierbei unterstützen könnten. Wäre es möglich, den angehängten Flyer mit dem unten stehenden Anschreiben, an Ihre StudentInnen und/oder Wissenschaftliche MitarbeiterInnen weiterzuleiten? Wir wissen, dass es schwierig sein könnte potentielle Teilnehmer kurz vor Weihnachten zu erreichen, jedoch können wir jede Unterstützung gebrauchen und würden uns über diese sehr freuen.

Wir bedanken uns im Voraus herzlich für Ihre Bemühungen und wünschen Ihnen erholsame und besinnliche Festtage.

Mit freundlichen Grüßen,
Clemens Bergmann und Gamze Canova

Text für Weiterleitung: Im Rahmen unserer Masterarbeit haben wir eine Spiele-App entwickelt, die fachfremde Benutzer über Internetsicherheit informiert. Diese App soll im Rahmen einer Benutzerstudie getestet werden. Hierzu brauchen wir deine Hilfe. Die Studie wird in Gruppen zu ca. 5 Personen in der zweiten Januarwoche (6.-10.) in Darmstadt stattfinden und insgesamt ca. 90 Minuten in Anspruch nehmen. Der/Die Beste der Gruppe gewinnt einen Amazon-Gutschein im Wert von 20€. Einzige Voraussetzung für die Teilnahme ist, dass du Erfahrung mit der Benutzung eines Smartphones hast. Bei Interesse oder Fragen erreicht ihr uns unter netstudy@cased.de.

Feindbild Internet?!

StudienteilnehmerInnen zur Internetsicherheit gesucht

Image courtesy of sheelamohan / FreeDigitalPhotos.net

TECHNISCHE UNIVERSITÄT DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

Im Rahmen unserer Masterarbeit haben wir eine Spiele-App entwickelt, die fachfremnde Benutzer über Internetsicherheit informiert.
Diese App soll im Rahmen einer Benutzerstudie getestet werden. Hierzu brauchen wir deine Hilfe.
Die Studie wird in Gruppen zu ca. 5 Personen in der zweiten Januarwoche (6.-10.) in Darmstadt stattfinden und insgesamt ca. 90 Minuten in Anspruch nehmen.
Der/Die Beste der Gruppe gewinnt einen amazon.de-Gutschein im Wert von 20€.
Einzige Vorraussetzung für die Teilnahme ist, dass du Erfahrung mit der Benutzung eines Smartphones hast.

Bei Interesse oder Fragen erreicht ihr uns unter netstudy@cased.de.

Internetsudie netstudy@cased.de
Internetsudie netstudy@cased.de
Internetsudie netstudy@cased.de
Internetsudie netstudy@cased.de
Internetsudie netstudy@cased.de
Internetsudie netstudy@cased.de
Internetsudie netstudy@cased.de
Internetsudie netstudy@cased.de
Internetsudie netstudy@cased.de
Internetsudie netstudy@cased.de
Internetsudie netstudy@cased.de

D.2 Explanatory Texts of Each Study Step

In order to ensure that the studies of small groups remain comparable we read all explanatory texts to the participants. This section provides a collection of these texts

D.2.1 Welcome and Introduction to Consent Form and General-Survey Before

Herzlich willkommen zu unserer Benutzerstudie. Danke, dass ihr euch die Zeit genommen habt uns zu unterstützen. Bitte bedient euch an den Süßigkeiten und dem Wasser auf den Tischen. Während der Studie werden wir die Erläuterungen vorlesen. Damit wollen wir sicherstellen, dass alle Durchläufe vergleichbar bleiben.

Wir würden euch gerne fragen, ob es in Ordnung für euch wäre, wenn wir das Gewinnspiel ein bisschen abändern: wir haben nämlich festgestellt, dass es in der Studie in Ausnahmefällen passieren kann, dass ihr nicht die gleichen Chancen habt zu gewinnen. Daher würden wir am Ende den Amazon-Gutschein gerne verlosen. Ist das für alle in Ordnung? Alles klar, super. Dann kanns weiter gehen.

In der Studie soll eine App getestet werden, die in Form eines Spiels Benutzern beibringen soll, wie sie sich besser vor Betrug im Internet schützen können. Um das Ganze ein bisschen spannend zu gestalten, wird am Ende die Person ermittelt, die hierbei am besten abgeschnitten hat. Ziel der Studie ist, die Wirksamkeit der App zu Testen. Hierzu haben wir folgenden Ablauf geplant: Keine Angst, ihr müsst euch nicht die einzelnen Schritte merken, wir erklären jedes mal was als nächstes kommt.

Als erstes bekommt ihr zwei Fragebögen ausgeteilt. Der Erste ist eine Einverständniserklärung, die ihr unterschreiben müsst, wenn ihr mitmachen wollt. Auf dem zweiten wird eure Selbsteinschätzung bzgl. eures Wissens zur Internetsicherheit abgefragt. Im zweiten Teil werden wir an Hand von Beispielen euer Vorwissen zum Thema Internetsicherheit genauer erfassen. Dies dient uns als Basiswert. Im dritten Teil werden wir euch Smartphones mit der App austeilen und ihr habt Zeit die App auszuprobieren. Dabei sammelt ihr bei dem Spiel Punkte, welche darüber entscheiden, wer von euch vieren das Spiel gewinnt. Dies wird die längste Zeit in Anspruch nehmen. Im vierten Teil werden wir euch erneut Beispiele zeigen, um zu erfassen, in wie weit, die App euch unterstützt. Im fünften Teil folgt eine "Freispielphase" in der ihr weitere Erfahrungen mit der App sammeln könnt. Im sechsten Teil folgt ein weitere Fragebogen zur allgemeinen Benutzbarkeit der App. Anschließend wird der Gewinner ermittelt und (der Amazon-Gutschein verlost) und damit ist die Studie auch beendet. Zuletzt würden wir uns freuen, wenn ihr noch einige Minuten für eine kurze offene Diskussionsrunde bleiben würdet, um eure Anmerkungen loszuwerden. Soviel zum Ablauf.

Bei Fragen oder Problemen mit der App meldet euch einfach und wir kommen zu euch um die anderen nicht unnötig zu stören. Wir werden euch bei technischen Problemen oder Bedienungsproblemen helfen. Inhaltliche Fragen können wir nicht beantworten weil dadurch der Einfluss der App auf euch nicht mehr geprüft werden könnte. Ihr habt jederzeit das Recht zu gehen und die Studie abzubrechen. Beachtet aber: Wenn ihr die Studie nicht vollständig mitmacht, könnt ihr natürlich nicht am Gewinnspiel teilnehmen.

Wichtig ist: Bitte bearbeitet alle Fragen und die App alleine. Ihr könnt nichts falsch machen. Beantwortet einfach alle Fragen nach besten wissen. Damit helft ihr uns am meisten. Wenn ihr mit dem Ausfüllen jeweils fertig seid gebt uns die Fragebögen einfach zurück. Habt ihr dazu noch Fragen?

Bevor es jetzt losgeht, wollten wir noch darauf hinweisen, dass die Studie ab jetzt ca. 1 Stunde dauern wird. Wegen des Studienaufbaus ist es leider nicht möglich sie zwischendurch kurz zu unterbrechen, daher nutzt jetzt bitte die Gelegenheit, falls ihr kurz raus müsst.

Ok, bevor es losgeht würden wir euch gerne darum bitten, eure Handys auf lautlos zu schalten und auch die Vibrati-

on auszustellen. Danke. Hier sind erst einmal die Einverständniserklärungen. Wenn ihr damit fertig seid, geben wir euch den zweiten Fragebogen.

D.2.2 Introduction to Website-Survey Before

Nachdem wir nun wissen was ihr vor dieser Studie über Internetsicherheit wusstet, können wir nun etwas konkreter werden. Bei der App handelt es sich um ein Spiel welches euch speziell Tips zum Thema Phishing gibt. Phishing ist ein Betrugsversuch. Hierbei spielt der Betrüger dem Benutzer vor jemand anderes zu sein. Das Ziel des Betrügers ist, dem Benutzer persönliche Informationen zu entlocken. Meistens macht er das über gefälschte Webseiten.

Im nächsten Fragebogen zeigen wir euch daher ein paar Webseiten. Ihr müsst entscheiden, ob diese gefälscht oder legitim sind. Für unsere Auswertung ist es wichtig, dass ihr die Seiten in der vorgegebenen Reihenfolge beantwortet und nicht zurück blättert, auch wenn euch im Nachhinein etwas auffällt. Schaut lieber zweimal hin.

D.2.3 Introduction to Playing App

So, jetzt ist die App an der Reihe. Wir teilen euch jetzt die Smartphones aus. Zusätzlich teilen wir euch einen Zettel aus. Darauf könnt ihr Anmerkungen zur App direkt notieren. Diesen könnt ihr bis zum Ende behalten und weiterhin Notizen darauf machen. Ihr könnt ihn dann am Ende mit dem letzen Fragebogen abgeben.

Jedes Telefon ist mit der Nummer eures Sitzplatzes beschriftet. Bitte verwendet nur euer Telefon. Auf dem Starbildschirm der Handys befindet sich die App. Sie heißt “NoPhish”. Wenn wir euch sagen, dass es losgeht, startet die App durch Antippen und wählt im Startmenü auf den grünen Button, um das Spiel zu starten. Ihr habt zum Spielen 30 Minuten zeit.

Im Laufe der App, werdet ihr nach eurer E-Mail Adresse gefragt. Dazu sind auf den Smartphones speziell für die Studie E-Mail Adressen angelegt worden. Diese werden euch bei der Eingabe in das Feld vorgeschlagen. Bitte wählt diese aus. Bei der Absender-Adresse dürft ihr eingeben, was ihr wollt.

Es ist nicht möglich die App in der Zeit vollständig durchzuspielen. Spielt einfach so weit ihr kommt. Wenn wir euch am Ende bescheid geben hört bitte einfach auf die App zu spielen und lasst sie so wie sie ist. Nur so können wir eure Punktzahl korrekt ablesen. Jetzt geht’s los. Viel erfolg.

D.2.4 Introduction to Website-Survey After and Further App Exploration

Die Zeit ist um. Bitte legt jetzt die Smartphones weg. Wir sammeln sie jetzt ein.

Jetz kommt nochmal ein Fragebogen mit Webseiten. Wie vorher sollt ihr darauf entscheiden ob eine Webseite gefälscht oder legitim ist. Wenn ihr damit fertig seid gebt den Fragebogen uns wieder zurück.

Jetzt teilen wir wieder die Smartphones aus. Wir bitten euch diesmal die anderen Funktionen der App auszutesten. Dafür habt ihr dann nochmal 5 Minuten.

D.2.5 Introduction to General-Survey After

Zum Schluss nochmal ein Fragebogen zur Benutzbarkeit. Wenn ihr damit fertig seid, gebt ihn bitte zusammen mit eurem Notizzettel wieder ab.

D.2.6 Issuance of Certificates, Debrief and Goodbye

Ihr habt es geschafft. Vielen Dank, dass ihr euch die Zeit genommen habt, die App zu testen. Haben sich bei euch noch Fragen ergeben?

Alles klar, dann kommen wir zur Bekanntgabe des Gewinners vom Spiel. Gewonnen hat <gewinnername/>, mit <gewinnerpunkte/> Punkten. Herzlichen Glückwunsch, du hast am besten abgeschnitten.

Nun kommen wir zur Verlosung des Amazon-Gutscheins. <name/> hat den Amazon-Gutschein gewonnen, herzlichen Glückwunsch.
<Erhaltbestätigung unterschreiben lassen/>

Allen anderen vielen Dank nochmal für eure Teilnahme.
<Austeilen der Anti-Phishing Awards>

Zum Schluss würden wir uns freuen, wenn ihr noch in einer kurzen Diskussionsrunde mitmachen würdet. Diese ist freiwillig. Wer möchte jetzt gerne gehen? Sehr schön, danke.

Die offene Diskussion würden wir gerne mit einem Diktiergerät aufzeichnen. Ist das für alle in Ordnung?

Nochmal vielen Dank an alle Teilnehmer. Wir hoffen es hat euch etwas Spaß gemacht und wünschen euch noch einen schönen Tag. Nehmt euch gerne noch Kekse und Gummibärchen für auf den Weg mit.

Tschüss

D.3 Study Forms

The following pages contain the forms as we used them in the user study. We did not include all example URL but only one exemplary page with an attacked URL.

Beginnfragebogen

1. Generelles	1.1. Datum	1.2. Uhrzeit	1.3. Platznr.

2. Einschätzungen

Im Folgenden sollst du entscheiden wie sehr du den entsprechenden Aussagen zustimmst.

	1 Stimme gar nicht zu	2	3	4	5 Stimme voll zu
2.1. Ich kenne mich gut genug aus, um den Gefahren im Internet aus dem Weg zu gehen.					
2.2. Es fällt mir leicht legitime von gefälschten E-Mails zu unterscheiden.					
2.3. Es fällt mir leicht legitime von gefälschten Webseiten zu unterscheiden.					
2.4. Sicherheit im Internet bezieht sich ausschließlich auf Finanzanwendungen.					
2.5. Persönliche Daten gebe ich im Internet nur an Anbieter weiter, die ich gut kenne.					
2.6. Mir persönlich ist es egal, was mit meinen persönlichen Daten im Internet geschieht.					
2.7. Für den Schutz vor Gefahren im Internet ist jeder selbst verantwortlich.					
2.8. Ich vertraue E-Mails, die von mir bekannten Personen oder Organisationen kommen.					

Beispiel-Webseiten

zur Studie

„Internetsicherheit“

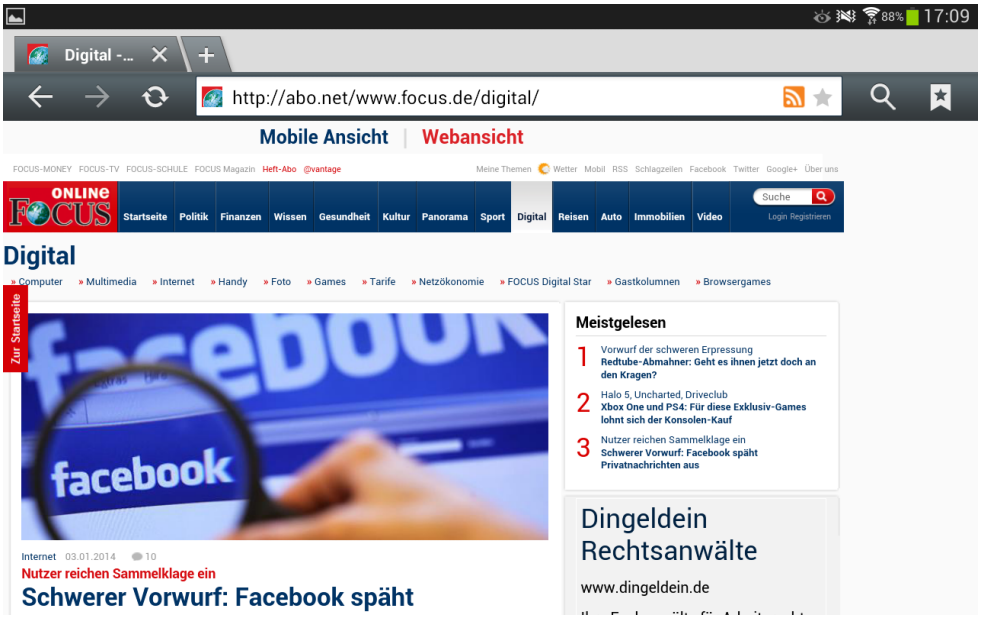
Datum:

Uhrzeit:

Sitzplatz:

OVorher ONachher

Bitte bearbeite diesen Fragebogen in der gegebenen Reihenfolge und blättere nicht zurück.



1. Würdest du auf dieser Webseite persönliche Daten eingeben?

O Ja O Nein

2. Umrande die Stelle, die dich am meisten zu deiner Antwort bewegt hat. Bitte markiere nur genau eine Stelle.

3. Wie sicher bist du dir?

Sehr unsicher O 1 O 2 O 3 O 4 O 5 sehr sicher

4. Kennst du „Focus“?

O Ja O Nein

5. Hast du bei diesem Anbieter ein Nutzerkonto?

O Ja O Nein

Abschlussfragebogen

1. Generelles

1.1. Datum	1.2. Uhrzeit	1.3. Platznr.

Zuerst ein paar generelle Fragen zu deiner Person.

1.4. Dein Alter....._____

1.5. Dein Geschlecht..... ☐Männlich ☐Weiblich ☐Anderes

1.6. Leidest du unter einer Farbenfehlsichtigkeit ? ☐Ja ☐Nein

1.7. Beruflicher Abschluss

☐Lehre ☐Meisterprüfung ☐Hochschulabschluss ☐Keiner ☐anderer: _____

1.8. In welchem Bereich arbeitest/studierst du zurzeit?....._____

1.9. Verwendest du ein Smartphone? ☐Nein ☐Ja, Android ☐Ja, iOS ☐Ja, _____

2. Benutzbarkeit

Im Folgenden sollst du entscheiden wie sehr du den entsprechenden Aussagen zustimmst. Es handelt sich hierbei um Standardfragen, daher kann es ggf. vorkommen, dass eine Aussage nicht ganz zutrifft.

	1 Stimme gar nicht zu	2	3	4	5 Stimme voll zu
2.1. Ich kann mir sehr gut vorstellen, die App regelmäßig zu nutzen.					
2.2. Ich empfinde die App als unnötig komplex.					
2.3. Ich empfinde die App als einfach zu nutzen.					
2.4. Ich denke, dass ich technischen Support brauchen würde, um die App zu nutzen.					
2.5. Ich finde, dass die verschiedenen Funktionen der App gut integriert sind.					
2.6. Ich finde, dass es in der App zu viele Inkonsistenzen gibt.					
2.7. Ich kann mir vorstellen, dass die meisten Leute die App schnell zu beherrschen lernen.					
2.8. Ich empfinde die Bedienung als sehr umständlich.					
2.9. Ich habe mich bei der Nutzung der App sehr sicher gefühlt.					
2.10. Ich musste eine Menge Dinge lernen, bevor ich mit der App arbeiten konnte.					

3. Meinung zur App

3.1. Der E-Mail Teil motiviert weiter zu machen.					
3.2. Die Menge der Texte war angemessen.					
3.3. Die Texte waren gut verständlich.					
3.4. Die App hat mir geholfen, Phishing Seiten zukünftig besser zu erkennen.					
3.5. Das Punktesystem mit den drei Leben pro Level war einfach zu verstehen.					

D.3.1 Example URLs of Website-Survey Before

- https://plus.google.com/u/0/me
- https://www.facebook.signin.com/Raumzeit
- http://m.youtube.com/watch?v=Ctzc8QSF6mQ
- http://www.amazon.de/Angebote/b/ref=cs_top_nav_gb27?ie=UTF8&
- http://130.83.162.6/wiki/Wikipedia:Hauptseite
- http://www.ebay.de/rpp/Deals/reisen-gutscheine/stadte-kultur/
- https://web.de.myponyfarm.com/
- http://abo.net/www.focus.de/digital/
- http://www.gmx.net/produkte/mail/promail/
- http://de.yahoo.com/?p=us
- https://www.ott0.de/damenmode/kategorien/anzuege-kostueme
- http://windows.mircosoft.com/de-de/windows/products
- http://badcat.com/mobile.twitter.com/session/new
- https://touch.www.linkedin.com/login.html
- http://m.spiegel.de/panorama/leute/a-937125.html#spRedir
- https://www.paypal-sicher.com/webapps/merchantboarding/web

D.3.2 Example URLs of Website-Survey After

- http://www.amazon.de/Angebote/b/ref=cs_top_nav_gb27?ie=UTF8&
- http://www.gutefrage.net.events-ma.de/tag/freizeit/1
- http://www.t-online.de/wetter/europawetter/64077226
- http://www.immobilienscout25.de/de/finden/wohnen/index.jsp
- http://www.ebay.de/rpp/Deals/reisen-gutscheine/stadte-kultur/
- http://de.yahoo.com/?p=us
- https://130.83.162.6/signup/
- https://plus.google.com/u/0/me
- http://abo.net/www.focus.de/digital/
- http://epaper.bild.de/
- https://www.facebook.signin.com/Raumzeit
- http://www.welt.de/sonderthemen/mittelstand/forschung/

- https://web.de.myponyfarm.com/
- http://windows.mircosoft.com/de-de/windows/products
- http://www.gmx.net/produkte/mail/promail/
- https://mail.live.dub123.com/login.srf?wa=wsignin1.0&rpsnv=12
- http://m.youtube.com/watch?v=Ctzc8QSF6mQ
- https://www.ott0.de/damenmode/kategorien/anzuege-kostueme/
- http://130.83.162.6/wiki/Wikipedia:Hauptseite
- https://www.paypal-sicher.com/webapps/merchantboarding/web
- https://touch.www.linkedin.com/login.html
- http://m.spiegel.de/panorama/leute/a-937125.html#spRedire
- http://badcat.com/mobile.twitter.com/session/new
- https://blog.xing.com/category/german/

D.4 Anti-Phish Certificates for Study Participants

Zertifikat

Die Arbeitsgruppe

SECUSO
SECURITY · USABILITY · SOCIETY

verleiht

hiermit den

GOLDEN ANTI-PHISH AWARD

Er/Sie hat bewiesen, dass er/sie sich erfolgreich vor den Phishing-Gefahren des Internets schützen kann.

Darmstadt, den _____

Studienleiter

Zertifikat

Die Arbeitsgruppe

SECUSO
SECURITY · USABILITY · SOCIETY

verleiht

hiermit den

SILVER ANTI-PHISH AWARD

Er/Sie hat bewiesen, dass er/sie sich erfolgreich vor den Phishing-Gefahren des Internets schützen kann.

Darmstadt, den _____

Studienleiter

References

[1] Global Finance. Internet users by country. http://www.gfmag.com/tools/global-database/ne-data/11942-internet-users.html#axzz2qr046GUb, 2012. Accessed: 2013-01-19.

[2] Norman M. Sadeh. Why phish should not be treated as spam. http://www.drdobbs.com/security/why-phish-should-not-be-treated-as-spam/240001777, 2012. Accessed: 2013-01-19.

[3] Anti-Phishing Working Group et al. Phishing activity trends report. *Anti-Phishing Working Group*, 2013.

[4] Kaspersky Lab. The evolution of phishing attacks: 2011-2013. *Kaspersky Lab*, 2013.

[5] RSA and ECM. Phishing kits - the same wolf, just a different sheep's clothing. *Fraud report*, 2013.

[6] Tyler Moore and Richard Clayton. How hard can it be to measure phishing? *Mapping and Measuring Cybercrime*, 2010.

[7] André Bergholz, Jan De Beer, Sebastian Glahn, Marie-Francine Moens, Gerhard Paaß, and Siehyun Strobel. New filtering approaches for phishing email. *Journal of computer security*, 18(1):7–35, 2010.

[8] Madhusudhanan Chandrasekaran, Krishnan Narayanan, and Shambhu Upadhyaya. Phishing email detection based on structural properties. In *NYS Cyber Security Conference*, pages 1–7, 2006.

[9] Ian Fette, Norman Sadeh, and Anthony Tomasic. Learning to detect phishing emails. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, pages 649–656, New York, NY, USA, 2007. ACM.

[10] Justin Ma, Lawrence K. Saul, Stefan Savage, and Geoffrey M. Voelker. Beyond blacklists: Learning to detect malicious web sites from suspicious urls. In *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '09, pages 1245–1254, New York, NY, USA, 2009. ACM.

[11] Jian Zhang, Phillip A Porras, and Johannes Ullrich. Highly predictive blacklisting. In *USENIX Security Symposium*, pages 107–122, 2008.

[12] Pawan Prakash, Manish Kumar, Ramana Rao Kompella, and Minaxi Gupta. Phishnet: Predictive blacklisting to detect phishing attacks. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–5, 2010.

[13] Ahmed Obied and Reda Alhajj. Fraudulent and malicious sites on the web. *Applied Intelligence*, 30(2):112–120, 2009.

[14] Samuel Marchal, Jérôme François, Thomas Engel, et al. Proactive discovery of phishing related domain names. In *Research in Attacks, Intrusions, and Defenses*, pages 190–209. Springer, 2012.

[15] Devdatta Akhawe and Adrienne Porter Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Proceedings of the 22th USENIX Security Symposium*, 2013.

[16] Tyler Moore and Richard Clayton. Examining the impact of website take-down on phishing. In *Proceedings of the Anti-phishing Working Groups 2Nd Annual eCrime Researchers Summit*, eCrime '07, pages 1–13, New York, NY, USA, 2007. ACM.

[17] Joris Evers. Security expert: User education is pointless. http://news.cnet.com/2100-7350_3-6125213.html, 2006. Accessed: 2013-01-29.

[18] Bruce Schneier. On security awareness training. http://www.darkreading.com/hacked-off/on-security-awareness-training/240151108, 2013. Accessed: 2013-01-29.

[19] Nermin Bajric. Cebit 2013 - user education not a cyber security starting point: Dsd. http://www.csoonline.com/article/734028/cebit-2013-user-education-not-a-cyber-security-starting-point-dsd, 2013. Accessed: 2013-01-29.

[20] SC Magazine. Weakest link: End-user education. http://www.scmagazine.com/weakest-link-end-user-education/article/161685/, 2010. Accessed: 2013-01-29.

[21] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Protecting people from phishing: The design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, pages 905–914, New York, NY, USA, 2007. ACM.

[22] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, pages 88–99, New York, NY, USA, 2007. ACM.

[23] Markus Jakobsson and Steven Myers. *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. Wiley. com, 2006.

[24] Phishing.org. Phishing techniques. http://www.phishing.org/phishing-techniques/. Accessed: 2013-01-19.

[25] Zulfikar Ramzan. *Phishing Attacks and Countermeasures*. Springer Berlin Heidelberg, 2010.

[26] Get Cyber Safe et al. Phishing: How many take the bait? http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx, 2012. Accessed: 2013-12-29.

[27] TrendLabs APT Research Team et al. Spear-phishing email: Most favored apt attack bait. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf, 2012. Accessed: 2013-12-29.

[28] Jason Hong. The state of phishing attacks. *Commun. ACM*, 55(1):74–81, January 2012.

[29] Dan Goodin. From phishing to whaling. http://www.theregister.co.uk/2008/04/16/whaling_expedition_continues/, 2008. Accessed: 2014-01-19.

[30] McAfee. The economic impact of cybercrime and cyber espionage. *Center for Strategic and International Studies*, 2013.

[31] RedCondor Secure. Phishing for disaster: the cost of corporate ignorance. *Whitepaper about the effects of corporate ignorance of phishing*, 2010.

[32] Mickey Boodaei. Mobile users three times more vulnerable to phishing attacks. http://www.trusteer.com/blog/mobile-users-three-times-more-vulnerable-to-phishing-attacks, 2011. Accessed: 2013-12-26.

[33] comScore Data Mine. Smartphones reach majority in all eu5 countries. http://www.comscoredatamine.com/2013/03/smartphones-reach-majority-in-all-eu5-countries/, 2013. Accessed: 2013-01-24.

[34] Microsoft. How to recognize phishing email messages, links, or phone calls. http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx. Accessed: 2013-01-11.

[35] PayPal. Was ist phishing? https://www.paypal.com/de/webapps/mpp/phishing. Accessed: 2013-01-11.

[36] eBay. GefÃďlschte e-mails erkennen und melden. http://pages.ebay.de/help/account/reporting-spoof.html. Accessed: 2013-01-11.

[37] Wombat Security Technologies. Anti-phishing phyllis. http://www.wombatsecurity.com/antiphishingphyllis. Accessed: 2013-01-11.

[38] SonicWALL. Sonicwall phishing iq test. http://www.sonicwall.com/furl/phishing/. Accessed: 2013-01-11.

[39] Microsoft. Identify fraudulent e-mail and phishing schemes. http://office.microsoft.com/en-001/outlook-help/identify-fraudulent-e-mail-and-phishing-schemes-HA001140002.aspx. Accessed: 2013-01-11.

[40] SPAMfighter. Becoming more difficult to detect phishing email attack, says security experts. http://www.spamfighter.com/News-18495-Becoming-More-Difficult-to-Detect-Phishing-Email-Attack-says-Security-Experts.htm, 2013. Accessed: 2013-01-11.

[41] Nalin Asanka Gamagedara Arachchilage, Steve Love, and Michael Scott. Designing a mobile game to teach conceptual knowledge of avoiding phishing attacksĂİ. *International Journal for e-Learning Security*, 2(2):127–132, 2012.

[42] PhishTank. Phishtank. http://www.phishtank.com/, 2013. Accessed: 2013-12-29.

[43] OnGuarOnline.gov. Phishing scams (game). http://www.onguardonline.gov/media/game-0011-phishing-scams. Accessed: 2013-01-11.

[44] Symantec. Race to stay safe. https://www.staysecureonline.com/staying-safe-online/. Accessed: 2013-01-11.

[45] Kenny. Jansson and Rossouw von Solms. Simulating malicious emails to educate end users on-demand. In *Web Society (SWS), 2011 3rd Symposium on*, pages 74–80, 2011.

[46] Ponnurangam Kumaraguru. *PhishGuru: a system for educating users about semantic attacks*. ProQuest, 2009.

[47] Melanie Volkamer, Simon Stockhardt, Steffen Bartsch, and Michaela Kauer. Adopting the cmu/apwg anti-phishing landing page idea for germany. In *3rd Workshop on Socio-Technical Aspects in Security and Trust (STAST), 2013*. IEEE Digital Library, June 2013.

[48] Nalin Asanka Gamagedara Arachchilage and Melissa Cole. Design a mobile game for home computer users to prevent from phishing attacks. In *Information Society (i-Society), 2011 International Conference on*, pages 485–489, 2011.

[49] ICICI Bank. The phishing game. http://www.icicibank.com/online-safe-banking/Phishing-Game.html. Accessed: 2013-01-17.

[50] Abdullah Alnajim and Malcolm Munro. An anti-phishing approach that uses training intervention for phishing websites detection. In *Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on*, pages 405–410, 2009.

[51] Anti-Phishing Working Group and CMU CUPS. Phishing education landing page project. *Anti-Phishing Working Group*, 2009.

[52] Sonia Chiasson, Manas Modi, and Robert Biddle. Auction hero: The design of a game to learn and teach about computer security. In *World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*, volume 2011, pages 2201–2206, 2011.

[53] OnGuarOnline.gov. Mission laptop security. http://www.onguardonline.gov/media/game-0008-mission-laptop-security. Accessed: 2013-01-17.

[54] OnGuarOnline.gov. Invasion of the wireless hackers. http://www.onguardonline.gov/media/game-0006-invasion-wireless-hackers. Accessed: 2013-01-17.

[55] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. Control-alt-hack: The design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 915–928, New York, NY, USA, 2013. ACM.

[56] Data Dealer. Data dealer. https://datadealer.com/de. Accessed: 2013-01-29.

[57] Chris Karlof, J Doug Tygar, and David Wagner. Conditioned-safe ceremonies and a user study of an application to web authentication. In *SOUPS*, 2009.

[58] IDC. Press release. http://www.idc.com/getdoc.jsp?containerId=prUS24442013, 2013. Accessed: 2013-01-24.

[59] Brightcove. Step-by-step guide to publishing in the apple app store using a mac. http://support.brightcove.com/en/app-cloud/docs/step-step-guide-publishing-apple-app-store-using-mac. Accessed: 2013-01-08.

[60] Brightcove. Step-by-step guide to publishing in the android market on windows. http://support.brightcove.com/en/app-cloud/docs/step-step-guide-publishing-android-market-windows. Accessed: 2013-01-08.

[61] Android. Android development - dashboards. http://developer.android.com/about/dashboards/index.html, 2013. Accessed: 2013-01-08.

[62] DIVSI - Deutsches Institut für Vertrauen und Sicherheit im Internet and Sozialwissenschaftliches Institut Nowak und Sörgel. *DIVSI-Milieu-Studie zu Vertrauen und Sicherheit im Internet: eine Grundlagenstudie*. Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI), 2012.

[63] Chaitrali Amrutkar, Patrick Traynor, and PaulC. Oorschot. Measuring ssl indicators on mobile browsers: Extended life, or end of the road? In Dieter Gollmann and FelixC. Freiling, editors, *Information Security*, volume 7483 of *Lecture Notes in Computer Science*, pages 86–103. Springer Berlin Heidelberg, 2012.

[64] Evgeniy Gabrilovich and Alex Gontmakher. The homograph attack. *Commun. ACM*, 45(2):128–, February 2002.

[65] Erik Larkin. Spot the tiny phishing trick. http://www.pcworld.com/article/161232/tinyphish.html, 2009. Accessed: 2013-12-29.

[66] Abdullah Alnajim. *Fighting internet fraud: anti-phishing effectiveness for phishing websites detection*. PhD thesis, Durham University, 2009.

[67] Wer zu Wem Firmenverzeichnis. Top 100 banken in deutschland. http://www.wer-zu-wem.de/ranking/banken/, 2011. Accessed: 2013-01-24.

[68] INTERNER WORLD Business. Ranking: Die 100 gröSSten online-shops in deutschland 2011. http://www.internetworld.de/Nachrichten/E-Commerce/Zahlen-Studien/Ranking-Die-100-groessten-Online-Shops-in-Deutschland-2011-Zalando-macht-zehn-Plaetze-gut-70245.html, 2011. Accessed: 2013-01-24.

[69] Curtiss Murphy. Why games work and the science of learning. In *Interservice, Interagency Training, Simulations, and Education Conference*, 2011.

[70] Edward L. Thorndike. *The fundamentals of learning.* Teachers College Bureau of Publications, 1932.

[71] Aviation Instructor's Handbook. Us dept of transportation. *Federal Aviation Administration*, 2008.

[72] Mihaly Csikszentmihalyi. Flow: The psychology of optimal performance, 1990.

[73] Martin EP Seligman. *Flourish: A visionary new understanding of happiness and well-being*. Simon and Schuster, 2012.

[74] Mihaly Csikszentmihalyi. *Finding flow: The psychology of engagement with everyday life*. Basic Books, 1997.

[75] Jesse Schell. *The Art of Game Design: A book of lenses*. Taylor & Francis US, 2008.

[76] Thomas Goetz. Harnessing the power of feedback loops. *Wired Magazine*, 19(07), 2011.

[77] Alison McMahan. Immersion, engagement and presence. *The video game theory reader*, pages 67–86, 2003.

[78] Barry Schwartz. *The paradox of choice*. HarperCollins, 2009.

[79] Raph Koster. *Theory of fun for game design*. O'Reilly Media, Inc., 2010.

[80] GOV.UK. Guerilla testing. `https://www.gov.uk/service-manual/user-centered-design/user-research/guerilla-testing.html`, 2013. Accessed: 2013-01-24.

[81] David Peter Simon. The art of guerilla usability testing. `http://www.uxbooth.com/articles/the-art-of-guerilla-usability-testing/`, 2013. Accessed: 2013-01-24.

[82] Robert Gunning. *The Technique of Clear Writing*. McGraw-Hill, New York, 1952.

[83] Rudolph Flesch. A new readability yardstick. *Journal of Applied Psychology*, 32(3):221–233, 1948.

[84] Toni Amstad. *Wie verständlich sind unsere Zeitungen?* Abhandlung: Philosophische Fakultät I. Zürich. 1977. Studenten-Schreib-Service, 1978.

[85] Leicht Lesbar. Testen sie ihren text. `http://leichtlesbar.ch/html/`. Accessed: 2013-01-28.

[86] Stilversprechend. Stilversprechend. `http://stilversprechend.de/index.html`. Accessed: 2013-01-28.

[87] Peter Schöll. Flesch-index berechnen. `http://www.fleschindex.de`. Accessed: 2013-01-28.

[88] John Brooke. Sus: A retrospective. *Journal of Usability Studies*, 8(2):29–40, 2013.

[89] Frank Wilcoxon. Individual comparisons by ranking methods. *Biometrics bulletin*, 1(6):80–83, 1945.

[90] Min Wu, Robert C Miller, and Simson L Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 601–610. ACM, 2006.

[91] Serge Egelman, Jennifer King, Robert C Miller, Nick Ragouzis, and Erika Shehan. Security user studies: methodologies and best practices. In *CHI'07 extended abstracts on Human factors in computing systems*, pages 2833–2836. ACM, 2007.

[92] Alexa The Web Information Company. Top sites in germany. `http://www.alexa.com/topsites/countries/DE`. Accessed: 2013-01-26.