Anti-Phishing Education App

Design, Implementation and Evaluation

Master-Thesis von Clemens Bergmann und Gamze Canova

Dezember 2013

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Fachbereich Informatik
Security, Usability and Society

Anti-Phishing Education App
Design, Implementation and Evaluation

Vorgelegte Master-Thesis von Clemens Bergmann und Gamze Canova

1. Gutachten: Professor Dr. Melanie Volkamer
2. Gutachten: Arne Renkema-Padmos

Tag der Einreichung:

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 29. Dezember 2013

(C. Bergmann)

Erklärung zur Master-Thesis

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

Darmstadt, den 29. Dezember 2013

(G. Canova)

Inhaltsverzeichnis

Zusammenfassung

...

1 Introduction

This chapter introduces the target of this work, which is to design, implement and evaluate an educational app. The app is supposed to help unexperienced users to detect phishing attacks. At first we are going to motivate the benefit of our work and how we envision our approach to achieve our goal. Next, we define our specific objectives and finally, we provide an overview of the following chapters.

1.1 Motivation

Introductory sentence...

1.1.1 Statistics of Phishing

Nowadays, a world without Internet is unimaginable for many people. However, it is undeniable that the Internet brings at least as much threats with it as it brings benefits. One major issue of today's digitalized world is phishing, which is also reflected by many statistics of various reports. According to the Anti-Phishing Working Group (APWG) about 40,000 unique phishing websites are detected each month [9]. 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 the number of users, who were subject to phishing attacks, was 19.9 million, in 2012-2013 the numbers climbed up to 37.3 million. In particular, every day about 100,000 Internet users are victims of phishing attacks, which is twice as many compared to the previous period of 2011-2012. An immense increase can also be observed in the number of unique sources (i.e. IPs) of attacks, which has tripled from 2012 to 2013 [12]. The number of target institutions also rose. While in 2011 the APWG counted about 500 target institutions, in the fist quarter of 2013 720 target institutions were identified [8]. Finally, the estimated worldwide costs caused by phishing are about $1.5 billion for the year 2012 [22].

1.1.2 Consequences of Phishing

Falling for a phishing attack has several consequences for the victim as well as for the target company or organization. Phishing is the practice of tricking users to disclose their personal data. That is to say, a possible consequence of falling for a phishing attack is identity theft. With the data unknowingly provided by the victims, the attacker can impersonate his victims. Financial loss is another problem resulting from phishing attacks. Not only users who are subject to phishing attacks can suffer financial loss, but also the institutions, organizations and companies targeted by the phisher can. Financial loss can be the result of users' banking accounts being plundered or increased support costs for the targeted institutions due to their customers who fell for an attack. Moreover, the targeted institutions may sustain a damaged reputation due to phishing attacks. Customers who actually became a victim of such a phishing attack will be displeased about the money or account loss and the resulting efforts they have to make in consequence of such an attack. Furthermore, they will tell other people about this displeasant experience. Finally, these victims will lose their trust in the institution targeted by the phiser. Moreover, they might lose confidence in eCommerce operations and the Internet in general.

1.1.3 Technical Solutions to Counter Phishing

Several technical solutions to counter phishing have already been suggested in literature [20]. In the following some of these solutions are briefly summarized.

Spam filters Not rarely, the phisher sends out a mass of emails to users which link to fake websites, where the users are lured to disclose their personal data. Consequently, one possible countermeasure to stop phishing is to filter these e-mails before they even reach the receiver. Various approaches for such spam filters do already exist [2, 4, 7], but also have their drawbacks. First, it is not possible to make sure that all users make use of such spam filters. Second, even if spam filters are used by the majority, one can not make sure that they are updated regurlarly. In addition, phishers are able to adapt to improved technology. Consequently, such filters can not assure 100% accuracy. On the one hand it is possible that phishing e-mails can make it through these filters. As a result, the user might still fall victim to such an attack. On the other hand there are legitimate e-mails which might not reach the user. This might result in a user's loss of confidence, which in turn can result in the user not making use of the spam filter anymore [17].

Blacklists Fake websites are a common way for phishers to get at users' data. Thus, another alternative to protect endagered users from phishing attacks is to restrict the access to such phishing websites with the aid of so called blacklists.

Here, the browsers hold a list of revealed phishing websites. If a requested URL is contained in such a blacklist the access to this website can be restricted or the user can be alerted about the phishing website. Several blacklisting approaches have been suggested in literature [14, 27]. The major downside of blacklists is that most of them work reactively. That is to say, there is a certain time frame where phishing websites are active without being blacklisted. In this time frame users can access these website without being warned or restricted and thus are vulnerable to fall for the attack. To resolve this problem multiple dynamic and predictive approaches have been proposed to restrict and/or warn the user from accessing phishing websites [19, 16]. Nevertheless, there is no flawless blacklisting approach, as there are always malicious websites which can bypass such protective systems. Moreover, these systems require a high effort, since a regular and realtime update is inevitable in order to make the system effective [20]. Finally, there is the weakest link in the security chain, the users who are very often unsure about what to do when getting such security warnings [1]. In case of disregard of these warnings such systems are useless.

Visual distinction A further technical approach against phishing is the visual distinction of phishing websites from legitimate ones. For this purpose it is necessary to identify malicously duplicated websites mainly based on visual similarities [13]. Various solutions can be found in literature to approach this [5, 6, 26]. However, there is no foolproof solution. In particular, if approaches rely on visual similarities many of them will fail if the phishing website is not a duplicate of the original site. Moreover, phishers will always be able to adapt to sophisticated solutions in order to bypass these security levels. Finally, as always the human factor plays a huge role here: if users keep misunderstanding or ignoring such visual security indicators such techniques will remain of no use.

Takedown Another possibility to protect users from accessing phishing websites it to take them down [15]. Here, hosting service providers are urged to take down such malicious websites by for example banks, other organizations or specialist takedown companies. In this way, a visitor will not see anything of the phishing website on this particular site and thus will not provide his data to the phisher. The removal of phishing website is an effective solution, since it implicitly solves the problem with the human factor, where users ignore security warnings. However, this approach can not defeat phishing completely, since it is not fast enough [15]. During the uptime of the fraudulent website falling for these attacks remains possible.

As a conclusion, there are two major issues of technical solutions. First, technical solutions do not assure 100% accuracy. There is always the potential of false positives and false negatives. Furthermore, attackers will find a way around sophisticated solutions and be able to bypass these somehow. The second major problem with these approaches is the user behavior. As indicated above users tend to overlook or intendedly ignore security warnings. If the user behavior does not change such approaches will remain useless. The main reason why users overlook or ignore such security indicators is that security is not their primary goal. Consequently, they give their attention to other things, for example, shopping, online banking and so on. Another factor for overlooking and ignoring these warnings is the lack of user awareness. Some users are just not aware of how easy it is for even unexperienced attackers to duplicate a website and send out fake e-mails. Even if users are aware that there is a certain degree of threat in the Internet, people tend to think the probability that they will face such an attack is very low and that it will not happen to them, until it happens to them. Thus, an important step towards changing the user behavior is increasing the user awareness.

1.1.4 Anti-Phishing Education on the Smartphone

There are several reasons why we chose to educate users on the smartphone. The main characteristic of a smartphone is that it is enormously smaller than the well-known desktop computers. As a consequence there is much less space in 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. There is also the fact that users often use their smartphones while on the move, for example, when walking, during a train or a bus ride. These circumstances include distractions from the environment which are unavoidable. These distractions obviously will influence the user's attentiveness. As a consequence smartphone users are even more vulnerable to phishing attacks than the traditional desktop user. This is also indicated by a report of 2011, which says that mobile users are three times more likely to access phishing websites than desktop users [3]. Evidently, there is a need for smartphone user protection. Additionally, educating the user on the smartphone provides two major benefits. First, the user can use the app on the move. Thus, the app is accessible outside of the user's desktop environment, where he potentially has better things to do than learning how not to fall for phishing attacks. The app can be used while train or bus rides, while waiting for a friend or while waiting for any other appointment. The app can be used any time as a sideline, so that probably more users would be willing to use it. Finally, to the best of our knowledge there does not exist a smartphone application to educate users about phishing yet.

1.2 Goals

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

1. Increasing the user awareness
2. Educating users about phishing

As already indicated in the previous section the lack of user awareness seems to be a major issue concerning the secure user behaviour. For this reason we want to raise the user awareness by showing our app users that faking e-mail senders and content is very easy. Additionally, we want to make them aware that links do not necessarily lead to the target the link displays to the user. This should happen at the beginning of the app so that the user realizes that the threat of the Internet is prevalent and that he needs to learn to protect himself. Furthermore, the user should practically experience these aspects and not only told, since being told will not suffice to motivate the user to go on with the app. Increasing the user awareness will not be enough to help the user not to fall for phishing attacks. Besides technical solutions valuable information has to be made available to the user. In particular, we want to qualify our app users to detect phishing URLs so they can distinguish phishing websites from legitimate ones.

1.3 Outline

This thesis consists of ... main chapters: .... Their purpose is as follows:
Chapter 1 motivates this work...
Chapter 2 ...
Chapter 3 ...
...
Chapter ... finally summarizes this work and provides an outlook on future work.

2 Background

Introducing sentences...

2.1 Definition of Phishing

The goal of this work is helping users to distinguish phishing websites from legitimate ones. Since phishing is important in the scope of this work, we are going to define the term first. The following definition is intendedly kept abstract.

"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, account information, and other personal information."

There exist several techniques how phishers can steal users' personal data. In the following section we dwell on some of these techniques.

2.2 Phishing Techniques

There are various possibilities how phishers can obtain users' confidential information. In the following we describe phishing techniques that can be distinguished [11].

Deceptive Phishing In deceptive phishing social engineering plays a decisive role. Here, users are lured to disclose 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. 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. 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. 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 in on a website of his trust, the entered information is actually transmitted to the phisher.

DNS Based Phishing This kind of phishing is also referred to as pharming and includes the manipulation of a system's host file or domain name system. 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 and can misuse them.

Man-in-the-Middle Phishing 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 Phishing Content injection phishing refers to the practice of embedding additional harmful content into legitimate websites. This content can, for example, be malvolent code to log users' sensitive information and deliver the input to the phishing server. Well-known types of content-injection phishing include, for example, cross-site scripting. Cross-site scripting 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 Phishing Other phishing attempts involve search engines. Here, websites with offers for fake low cost products and/or services are legitimately indexed with search engines. Thus, users reach these websites when using the search engine. These offers, which are often too good to be true, then lure the user to buy those fake products which in turn leads to the disclosure of their sensitive information, such as the credit card number, to the phisher.

Within the scope of this work we focus on deceptive phishing. In particular, we target the detection of phishing websites resp. phishing URLs. Besides the different kinds of techniques of phishing there also exist a number of attack channels a phisher can make use of. The following section deals with these attack channels.

2.3 Phishing Attack Channels

Several attack channels that can be used by phishers to reach their victims. This section intends to introduce possible attack channels [21].

E-Mail E-Mail spoofing is a common way of a phisher to reach his victims. These e-mails usually imitate renowned institutions, organizations, companies or banks the recipients trust. They usually contain a text which will deceive the recepient into doing what it says. Usually these e-mails link to a malicious website, whose look and feel is almost identical to the original one. There the user is lured to enter his sensitive data which is captured by the phisher. Other alternatives are embedded forms in the e-mail the user has to fill in. 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 to divulge his sensitive information. The user may also be asked to send back the information directly. Another possibility is to be asked to call back a fraudulent telephone number indicated in the short message. 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 In this attack the user receives an instant message from one of his friends. However, the user does not know that his friend's account has been compromised by a phisher. The message usually contains a link to a website asking the user for his instant messenger account information (user name and password). As the link came from a friend many users do not expect something harmful behind this and thus enter their credentials. When the phisher acquires the user's credentials he can continue playing this game with the friends of the user's instant messaging account which has just been compromised.

Online Social Networks Using online social networks works as 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. Consequently, the likelihood for his targets to get phished increases.

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 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 tricked to disclose confidential information. Alternatively, the phisher can directly call the user and lure him into divulging his senstitive information. With Voice-over-IP (VoIP) these kind of attacks are executable easily and inexpensivly. Voice Phishing is also referred to as Vishing.

In the scope of our work we focus on the detection of spoofed websites resp. phishing URLs. Phishing websites can be reached in several ways. Links to fake websites are usually distributed via e-mails, instant messages or online social

networks. However, they can also be spread via SMS or even phone calls. Ultimately, a phishing website can also be reached by just surfing in the Internet. As a consequence, our approach covers all attack channels, as long as the user is tricked to divulging sensitive information via a phishing website.

2.4 Variations of Phishing

In the course of time different variations of phishing have evolved. This section deals with some of these variations that can be found in literature. Do we need this subsection?

Mass Phishing Here, for example, the phisher 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 to disclose their credentials. 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. 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 [23].

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, knowledge of the targeted individuals and organizations is used. Usually, victims of spear phishing receive e-mails with a malicious attachment and are lured to download it. 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 legitimate context. This makes spear phishing attacks very hard to detect[25, 10].

Whaling Whaling is a specific form of spear phishing. The target distinguishes whaling from spear phishing. While spear phishing aims at specific individuals or groups within organizations, whaling attacks are after high-level targets, such as senior executives or other leaders in positions of influence.

We cover in particular mass phishing. However, the URL checking can be applied in case of any variant, as long as the attack includes a website which lures the user to type in his credentials. In the following section we will summarize and reason the scope of phishing we are going to cover in this work.

2.5 Scope

In the previous sections we have introduced numerous phishing techniques, attack channels as well as phishing variations. As there are more ways of how phishing can be understood, we have to constrain the scope of the term phishing for this work. In literature most of the time phishing is described as the act of gaining sensitive information with the aid of fake websites which trick unsuspecting users into disclosing their credentials. This type of attack is a form of deceptive phishing. For this reason we have 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. As our focus will be set on the analysis of URLs, it does not matter where these links came from. Any attack channel distributing a link to a fake website will be covered by our approach. Finally, there are three variations of phishing we have introduced. Our main focus is the mass phishing attack. However, if any spear phishing or whaling attack should involve fake websites, this would be covered by our approach also.

3 Related Work

In the following, we present a survey of approaches to anti-phishing education.... We divided the related work we have found in literature into two categories: the *content*, i.e. what the user is taught and the *medium*, i.e. how the user is taught.

3.1 Content Classification

General Knowledge Transfer

E-Mail Based Knowledge

URL Based Knowledge

3.2 Medium Classification

Game Based Learning

Quiz Based Learning

Comparison Based Learning

Emdedded Learning

3.3 Previous Work

Previous work here ... (e.g. Anti-Phishing Phil and Phyllis)

4 Focus

Introductory sentences...

4.1 Focus

Based on the discussion of the previous section we decided to.....

4.2 System Requirements

Android OS

Version

Android Standard Browser (transfer of knowledge to other browsers possible)

4.3 Assumptions

Secure DNS ...

Secure Smartphone ...

No Before-Click URL Analysis ...

Download URLs Possible ...

4.4 Limitations of Our Approach

Cross-Site Scripting ...

URL Hiding Techniques ...

5 Target Group

Introductory sentences... DIVSI

6 Pre-Survey

Introductory sentences...

6.1 Main Objective

6.2 Survey Details

6.3 Evaluation

7 Teaching and Learning Content

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

7.1 Phishing URLs

As aforementioned, we focus on teaching the user how to analyze a given URL and to decide on it 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 how the URLs are spoofed in order to deceive the users. For the analysis of phishing URLs we chose the database of PhishTank. 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. Renowned organizations such as Yahoo, Kaspersky Lab and Mcafee use the data submitted by PhishTank [18]. A further deciding reason to choose PhishTank as our phishing URL database was that Kaspersky Lab itself recommended us to make use of it for our URL analysis. For the phishing URL analysis we made use of the URL categories which had been identified by the authors of Anti-Phishing Phil [24] as a starting point. To these belong IP address URLs, subdomain URLs as well as similar and deceptive domain URLs. With these given categories we tried to assign the PhishTank URLs to the available 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 URL in the PhishTank database. In the following the identified URL categories are explained.

7.1.1 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 about the authenticity of an URL when it contains the brand name anywhere. Phishers exploit this lack of knowledge in different way. In the following we present the identified spoofing attacks on URLs and state whether they are covered by the app.

Subdomain Phishers make use of subdomains which are very similar or even identical to the domains of the spoofed target institutions. This makes the users believe that they are on a legitimate website. This form of URL spoofing is covered by our education app.

IP Address Sometimes phishers do not even bother registering any domain at all. In this case, the URL to the phisher's fake website contains an IP address. This form of URL spoofing is covered by our education app.

Nonsense Domain We frequently encountered URLs which had registered quite nonsense as their domain. The domain names ranged from random letters to domain names like "marketstreetchippy.com". Sometimes other parts of the URL contained the brand name, but sometimes there was no clue in the URL about to where it is actually leading. This form of URL spoofing is covered by our education app.

Trustworthy, But Unrelated Domain Some URLs are very well-crafted. When reading them they appear meaningful and trustworthy. This is particularly accomplished by making use of domain names which sound very trustworthy, for example, "account-information.com", "secure-login.de" or "security-update.com". If the URL additionally contains the brand name of the target institution somewhere in the URL the user can be perfectly deceived. This form of URL spoofing is covered by our education app.

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 has 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. This form of URL spoofing is covered by our education app.

Homograph Attack 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 langauge sets, such as Cryllic languages, where the characters will look almost identical [**?**]. The letter case is indistinguishable for the human eye in many cases. 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 URL 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. 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 it quite popular [**?**]. Tiny URLs redirect the tiny URL to the actual long URL. 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"[?]. 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 tiny URL to be covered by the app.

7.1.2 Problems and Challenges With The Categorization

7.2 Android Elements

Eventuell Titel umbenennen, anders strukturieren...

Invisible Address Bar Find URL Bar, Browser

Use of Https Within Websites Browser

Analyze Complete URL Via Address Bar Browser

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

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

7.3 Android Browser Security Indicators

Https Padlock Browser

Displayed Webaddress on Https Sites Browser

Certificate Verification

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

7.4 E-Mail Spoofing

From Field not trustworthy

E-Mail Content in hand of attacker

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

7.5 General Recommended Behavior

Do Not Click

Do Not Download Attachment

Look at URL

Data Economy

Date Entry Via Https

7.6 Conclusion / Summary

Summarize what to communicate to user here...

8 Approach for Our Anti-Phishing Education App

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

8.1 App Design

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

8.2 Game Rules

8.3 Leveling Strategy

Three approaches...

8.4 Knowledge Transfer Per Level

What is taught in each level ...

8.5 URL Generation

8.6 Gamification

User motivation

Show Leaderboard Rate

Show Leaderboard Total

...

9 Evaluation

The goal of this chapter is to evaluate our Anti-Phishing Education App which we described in the previous chapter.

9.1 Hypotheses

9.2 Measurement

9.3 Participant Recruitment

9.4 Study Design

9.5 Results and Analysis

9.6 Discussion

9.7 Conclusion

10 Conclusion

This chapter provides a short summary of what we achieved in the scope of this thesis and presents an outlook on future work.

10.1 Conclusion

The objectives of this thesis...

10.2 Findings

10.3 Recommendations

10.4 Future Work

This section deals with a prospect on future work for our Anti-Phishing Education App. In particular, we present ideas that might be beneficial and which we were not able to realize due to time and resource limitations.

References

[1] T. Bakhshi, M. Papadaki, and S. Furnell. Social engineering: assessing vulnerabilities in practice. *Information management & computer security*, 17(1):53–63, 2009.

[2] A. Bergholz, J. De Beer, S. Glahn, M.-F. Moens, G. Paaß, and S. Strobel. New filtering approaches for phishing email. *Journal of computer security*, 18(1):7–35, 2010.

[3] M. 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.

[4] M. Chandrasekaran, K. Narayanan, and S. Upadhyaya. Phishing email detection based on structural properties. In *NYS Cyber Security Conference*, pages 1–7, 2006.

[5] K.-T. Chen, J.-Y. Chen, C.-R. Huang, and C.-S. Chen. Fighting phishing with discriminative keypoint features. *Internet Computing, IEEE*, 13(3):56–63, 2009.

[6] T.-C. Chen, S. Dick, and J. Miller. Detecting visually similar web pages: Application to phishing detection. *ACM Trans. Internet Technol.*, 10(2):5:1–5:38, June 2010.

[7] I. Fette, N. Sadeh, and A. 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.

[8] A.-P. W. Group et al. Apwg global phishing survey. *Anti-Phishing Working Group*, 2013.

[9] A.-P. W. Group et al. Phishing activity trends report. *Anti-Phishing Working Group*, 2013.

[10] J. Hong. The state of phishing attacks. *Commun. ACM*, 55(1):74–81, Jan. 2012.

[11] M. Jakobsson and S. Myers. *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. Wiley. com, 2006.

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

[13] W. Liu, X. Deng, G. Huang, and A. Fu. An antiphishing strategy based on visual similarity assessment. *Internet Computing, IEEE*, 10(2):58–65, 2006.

[14] J. Ma, L. K. Saul, S. Savage, and G. 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.

[15] T. Moore and R. 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.

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

[17] C. K. Olivo, A. O. Santin, and L. S. Oliveira. Obtaining the threat model for e-mail phishing. *Applied Soft Computing*, 2011.

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

[19] P. Prakash, M. Kumar, R. Kompella, and M. Gupta. Phishnet: Predictive blacklisting to detect phishing attacks. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–5, 2010.

[20] S. Purkait. Phishing counter measures and their effectiveness–literature review. *Information Management & Computer Security*, 20(5):382–420, 2012.

[21] Z. Ramzan. *Phishing Attacks and Countermeasures*. Springer Berlin Heidelberg, 2010.

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

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

[24] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. 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.

[25] T. A. R. 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.

[26] H. Zhang, G. Liu, T. W. S. Chow, and W. Liu. Textual and visual content-based anti-phishing: A bayesian approach. *Neural Networks, IEEE Transactions on*, 22(10):1532–1546, 2011.

[27] J. Zhang, P. A. Porras, and J. Ullrich. Highly predictive blacklisting. In *USENIX Security Symposium*, pages 107–122, 2008.