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 26. 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 26. 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 [10]. 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 [18].

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 [17]. 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 [15].

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 [12, 20]. 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 [16, 14]. 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 [17]. 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 [11]. Various solutions can be found in literature to approach this [5, 6, 19]. 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 [13]. 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 [13]. 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

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

"Definition of Phishing"

The next section dwells on different phishing types.

2.2 Phishing Techniques

In this section we are going to describe the different phishing techniques that are distinguished in literature. Furthermore we state and reason which technique(s) of phishing we focus on in our work.. Phishing techniques include, but are not limited to:

Deceptive Phishing

Malware Based Phishing (including keyloggers and screenloggers)

Host File Poisoning

DNS Based Phishing (Pharming)

Man-in-the-Middle Phishing

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

2.3 Phishing Attack Channels

E-Mail

SMS

Instant Messaging

Online Social Networks

Fake Website

VoIP

Malicious Downloads

We focus on fake websites. Usually, the links to fake websites are distributed via e-mails, SMS, instant messengers or online social networks, Thus, our approach automatically covers the attack channels e-mail, sms, instant messaging and online social networks.

2.4 Variations of Phishing

Do we need this subsection?

Mass Phishing

Spear Phishing

Persistent Spear Phishing

Clone Phishing

Whaling

We cover in particular mass phishing. However, the URL checking can be applied in case of any variant, as long as the attack is executed via a fake website.

2.5 Scope

3 Related Work

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

3.1 Content Classification

General Knowledge Transfer

E-Mail Based Knowledge

URL Based Knowledge

3.2 Medium Classification

Game Based Learning

Quiz Based Learning

Comparison Based Learning

Emdedded Learning

3.3 Previous Work

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

4 Focus

Introductory sentences...

4.1 Focus

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

4.2 System Requirements

Android OS

Version

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

4.3 Assumptions

Secure DNS ...

Secure Smartphone ...

No Before-Click URL Analysis ...

Download URLs Possible ...

4.4 Limitations of Our Approach

Cross-Site Scripting ...

URL Hiding Techniques ...

5 Target Group

Introductory sentences... DIVSI

6 Pre-Survey

Introductory sentences...

6.1 Main Objective

6.2 Survey Details

6.3 Evaluation

7 Teaching and Learning Content

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

7.1 Phishing URLs

Focus on distinguishing phishing URLs from legitimate ones.

7.1.1 Phishing URL Categorization

Potential phishing URL categories/phishing attcks on URLs

Subdomain covered

IP Address covered

Nonsense Domain covered

Trustworthy, But Unrelated Domain covered

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

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

Tiny URLs Not covered

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

Encoding Tricks Not covered - because redirect

7.1.2 Problems and Challenges With The Categorization

7.2 Android Elements

Eventuell Titel umbenennen, anders strukturieren...

Invisible Address Bar Find URL Bar, Browser

Use of Https Within Websites Browser

Analyze Complete URL Via Address Bar Browser

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

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

7.3 Android Browser Security Indicators

Https Padlock Browser

Displayed Webaddress on Https Sites Browser

Certificate Verification

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

7.4 E-Mail Spoofing

From Field not trustworthy

E-Mail Content in hand of attacker

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

7.5 General Recommended Behavior

Do Not Click

Do Not Download Attachment

Look at URL

Data Economy

Date Entry Via Https

7.6 Conclusion / Summary

Summarize what to communicate to user here...

8 Approach for Our Anti-Phishing Education App

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

8.1 App Design

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

8.2 Game Rules

8.3 Leveling Strategy

Three approaches...

8.4 Knowledge Transfer Per Level

What is taught in each level ...

8.5 URL Generation

8.6 Gamification

User motivation

Show Leaderboard Rate

Show Leaderboard Total

...

9 Evaluation

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

9.1 Hypotheses

9.2 Measurement

9.3 Participant Recruitment

9.4 Study Design

9.5 Results and Analysis

9.6 Discussion

9.7 Conclusion

10 Conclusion

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

10.1 Conclusion

The objectives of this thesis...

10.2 Findings

10.3 Recommendations

10.4 Future Work

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

References

[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 Transactions on Internet Technology (TOIT)*, 10(2):5, 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*, pages 649–656. ACM, 2007.

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

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

[12] 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*, pages 1245–1254. ACM, 2009.

[13] 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*, pages 1–13. ACM, 2007.

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

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

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

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

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

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

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