NoPhish: An Anti-Phishing Education App*

Gamze Canova, Melanie Volkamer, Clemens Bergmann, and Roland Borza

Technische Universität Darmstadt name.surname@cased.de

Abstract Phishing is still a prevalent issue in today's Internet. It can have financial or personal consequences. Attacks continue to become more and more sophisticated and the advanced ones (including spear phishing) can only be detected if people carefully check URLs. We developed a game based smartphone app – *NoPhish* – to educate people in accessing, parsing and checking URLs; i.e. enabling them to distinguish trustworthy and non-trustworthy websites. Throughout several levels information is provided and phishing detection is exercised.

1 Introduction

The financial benefit of phishing [1] is an incentive for phishers to keep luring victims into disclosing their sensitive information. The anti-phishing working group registered more than 100.000 unique phishing attacks in the second half of 2013, i.e. impersonated websites [2]. Furthermore, they report that the average up-time of such websites is about 28 hours. During this time potential victims are still likely to fall for an attack. People could be supported by tools such as the Netcraft Extension. However, such tools can never provide 100% accuracy [3]. Therefore, the tools' checks need to be complemented by humans checking the URLs. Many people lack the required knowledge to properly check URLs [4,5] and assess the trustworthiness of a given website. Some people are not even aware of faked messages and websites at all [6,4]. Several solutions have been proposed to address the problem of lacking knowledge e.g. tutorials or guides[1], quizzes[2] and games[3,4]. Tutorials are read-intensive if they cover all the different channels (such as email or SMS) and URL spoofing tricks phishers exploit. The quizzes – if at all – do not explain why answers are correct/incorrect. The game Anti-Phishing Phyllis only focuses on the email channel. Anti-Phishing Phil 1 and 2 [3] are already rather advanced in terms of different URL spoofing tricks; but can still be improved by including awareness aspects, addressing different channels, explaining the structure of a URL more precisely, addressing more categories of URL spoofing tricks, and providing knowledge about HTTPS.

*Long version available on request

[1] https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/phishing_node.html

[2] https://www.staysecureonline.com/staying-safe-online/

[3] http://www.wombatsecurity.com/antiphishingphyllis

[4] http://jackieweber.net/Projects/phil.html

Our goal was to develop a new game – *NoPhish* – an anti-phishing education app that addresses these issues to provide more sophisticated knowledge on how to properly check URLs. We opted for an Android smartphone app since in particular smartphone users are more likely to access phishing websites than desktop users. We decided to focus on the mobile browser rather than checking URLs before clicking on a link, e.g. with the aid of a preview function. Checking the URL previews would have the advantage that phishing could be detected before even clicking on a link. Yet, well-crafted URLs can still deceive users because URL previews are cropped in case they are too long. Additionally, not all email clients offer the preview functionality, e.g. Android's standard email client (e.g. version 4.4.2). We applied several learning principles [7], such as exercise, effect and primacy, to optimize learning effects. Gamification elements[5] like lives, levels, achievements, and leaderboards were also implemented to increase motivation. We followed a user-centered design, including an initial user survey to get an idea of the users' preferences with regard to an educational app. The results of our survey confirmed previous findings by Volkamer et al. [8] that for a German audience (adults at least) a rather neutral game based approach would be best accepted. Furthermore, we involved potential users in early stages by asking them to evaluate app texts before integrating them into the final game.

2 Game Design

The app entails two introductory parts and the game with ten levels mainly covering URL spoofing tricks.

2.1 Introduction Parts

Part 1 - Raise awareness of spoofed messages, links, and websites: First, users are made aware of how simple it is to spoof messages. This is done by enabling them to send themselves with the *NoPhish* app an email from a sender address they provide in a corresponding form; and with a content they provide there as well. After submitting the form, *NoPhish* requests the users to check their email inbox. The sender of the received email is the one just chosen by the user. Furthermore, the email contains a link with the displayed text "https://www.google.de/" and users are asked to follow the link to search for "Phishing". However, clicking on this link redirects the users back to the app. Thereby, users learn by experience that they should not trust displayed link texts. At the end the user is told that faking websites is simple as well. Finally, in the app the user is informed that this kind of forgery is not only possible with emails, but also with, e.g. social networks, SMS or instant messaging systems.

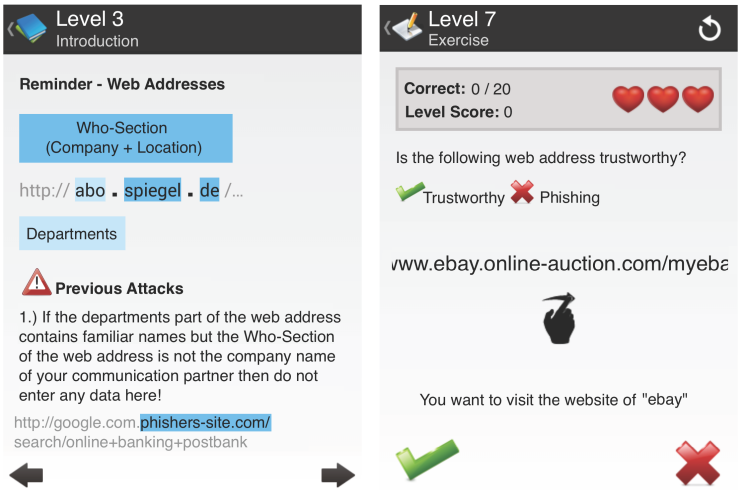
Part 2 - Access address bar and view entire URL: Due to the lack of space a mobile browser generally hides the address bar with its URL. Furthermore, the

[5] `http://badgeville.com/wiki/Game_Mechanics`

URL has to be scrolled in order to entirely view it. This part teaches the users how to access and view the entire URL in the mobile browser. The explanations how to do so are supported with corresponding screenshots. This part includes an exercise. Here, users are required to access the URL of a website they are forwarded to by *NoPhish*. Note, forwarding happens in a way that users first have to scroll up (which is necessary to make the generally hidden address bar of a mobile browser reappear). On top of the page, there is a text field, where they are asked to enter the last four characters of the URL. Then, they are asked to identify the first word of the URL (check one out of four provided possibilities). Once submitted the app checks the users' answers and can thereby ensure that they managed to access and view the entire URL. The users are forwarded to *NoPhish* as soon as they successfully complete the exercise.

2.2 Gaming Part

The gaming part is split into ten levels with increasing difficulty. Each level consists of two parts: an introductory block and the actual exercise. For the introduction of URL spoofing tricks the introductory block consists of a reminder, which provides a summary of previous levels (cf. Figure 1(a)) and the introduction of a new URL spoofing trick. The exercise is designed in a playful manner,



(a) Reminder (b) Exercise - Phish/No Phish

Figure 1: NoPhish Screenshots

i.e. users start with three lives, represented by hearts, and can collect points for correct answers and lose points and lives for wrong ones. Users receive direct feedback on their decision, e.g. they are immediately told why their answer was wrong. The next level is achieved if and only if a predefined amount of phishing and legitimate URLs have correctly been identified. To simulate the "behavior" of the address bar in mobile browsers, the entire URL as such is not displayed

but only parts of it. The user needs to scroll to the start of the URL in order to decide about the legitimacy of the displayed URL (cf. Figure 1(b)).

Level 1 - Structure of a URL: It is essential for people to achieve the capability of parsing a URL properly before learning different URL spoofing tricks. Especially the identification of the domain (first- and second-level domain) in a given URL is a key aspect which needs to be covered extensively. Therefore, the users start learning to identify the domain of a URL in level 1. To explain the different parts, we do not use technical terms such as URL, domain, subdomain, protocol and only provide details users need to know to successfully detect phishing URLs. The focus of this level is the domain, the *Who-Section* as we refer to it in *NoPhish*. During the exercise the users are asked to tap on the *Who-Section*.

Levels 2-8 - URL spoofing tricks: In levels 2-8 various URL spoofing tricks (cf. Table 1) are addressed. In level 2, we also explain IP addresses by using the analogy of house addresses. During the exercises, URLs together with the name of the website the users are supposed to visit are displayed (cf. Figure 1(b)). Users are asked to decide whether the URLs are legitimate or phishing ones. The URLs where selected from the top Alexa domains for Germany. The corresponding attack was then applied to a legitimate URL from the set whenever needed. Note, that in all levels both, HTTP and HTTPS URLs are displayed to the user, i.e. legitimate as well as phishing URLs can use HTTPS. Everytime the users correctly identify a phishing URL, *NoPhish* asks them to tap on the *Who-Section*. Depending on how often the user correctly identifies the Who-Section the frequency of asking to tap on the *Who-Section* decreases or increases.

URL Spoofing Tricks	**Level**
a) IP address, no brand (e.g. http://130.82.162.6/)	Level 2
b) Random/unrelated/trustworthy domain, no brand (e.g. https://marketchippy.com/ or http://www.account.com/login)	Level 3
c) Random/unrelated/trustworthy domain, brand in subdomain (e.g. http://paypal.kjdhsbc.com/signin)	Level 4
d) Random/unrelated/trustworthy/IP domain, brand in path (e.g. http://online-payment.com/www.paypal.com/)	Level 5
e) Derivated domains (e.g. https://www.facebook-login.com/)	Level 6
f) Introducing typos (e.g. http://www.twittter.com/)	Level 7
g) Replacing Character(s) (e.g. http://www.arnazon.com/)	Level 8

Table 1: URL Spoofing Tricks – Levels – Assignment

Level 9 - HTTPS: In this level, we introduce and explain the difference between HTTP and HTTPS. This level also includes an exercise.

Level 10 - Final remarks: Here, users are made aware of some special cases: E.g. it is not generally secure to arbitrarily click on links as they could download malicious software. Additionally, the users are informed about further potential URL

spoofing tricks that have not been exercised: e.g. homograph attacks. Also, the users are explained that they might encounter URLs which look very phishing-like, but actually are legitimate, e.g. https://www.paypal-community.com. Finally, *NoPhish* briefly introduces extended validation certificates.

3 Conclusion and Future Work

In the scope of this work, we have designed and implemented an anti-phishing education app – *NoPhish*. The detection of phishing URLs is realized as a game, where the user can win or lose points or lives. We already conducted a user study which showed very promising results. However, as knowledge retention is essential, we intend to run a corresponding retention study in three months with the same participants. We plan to publish the results of both parts of the study together. In future, we also plan to assess how such an education app can best be distributed. An idea would be to utilize embedded learning [9] where simulated phishing emails are sent to users. Whenever users fall for such an email they could be proposed to download the education app. Furthermore, the game could be extended by asking users to build legitimate or phishing URLs themselves. *NoPhish* is available upon request as it still in the user study stage. Once the user study is completed and new findings are integrated we plan to publish *NoPhish* in the Google Playstore.

Acknowledgements. This work was supported by CASED and EC SPRIDE.

References

1. Ramzan, Z.: Phishing attacks and countermeasures. In: Handbook of Information and Communication Security. Springer (2010) 433–448
2. Aaron, G., Rasmussen, R., Routt, A.: Global phishing survey: Trends and domain name use in 2h2013. Anti-Phishing Working Group (2014)
3. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E.: Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In: SOUPS, ACM (2007) 88–99
4. Dhamija, R., Tygar, J.D., Hearst, M.: Why phishing works. In: SIGCHI, ACM (2006)
5. Lin, E., Greenberg, S., Trotter, E., Ma, D., Aycock, J.: Does domain highlighting help people identify phishing sites? In: SIGCHI, ACM (2011) 2075–2084
6. Li, T., Han, F., Ding, S., Chen, Z.: Larx: Large-scale anti-phishing by retrospective data-exploring based on a cloud computing platform. In: ICCCN, IEEE (2011) 1–5
7. Thorndike, E.L.: The fundamentals of learning. Teachers College Bureau of Publications (1932)
8. Volkamer, M., Stockhardt, S., Bartsch, S., Kauer, M.: Adopting the cmu/apwg anti-phishing landing page idea for germany. In: STAST, IEEE (2013) 46–52
9. Jansson, K., von Solms, R.: Simulating malicious emails to educate end users on-demand. In: Web Society (SWS), 2011 3rd Symposium on. (2011) 74–80