Learn to Spot Phishing URLs with the Android NoPhish App

Gamze Canova, Melanie Volkamer, Clemens Bergmann, Roland Borza, Benjamin Reinheimer, Simon Stockhardt, Ralf Tenberg

▶ **To cite this version:**

Gamze Canova, Melanie Volkamer, Clemens Bergmann, Roland Borza, Benjamin Reinheimer, et al.. Learn to Spot Phishing URLs with the Android NoPhish App. 9th IFIP World Conference on Information Security Education (WISE), May 2015, Hamburg, Germany. pp.87-100, 10.1007/978-3-319-18500-2_8 . hal-01334293

HAL Id: hal-01334293
https://hal.science/hal-01334293

Submitted on 20 Jun 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Learn To Spot Phishing URLs with the Android NoPhish App

Gamze Canova, Melanie Volkamer, Clemens Bergmann, Roland Borza, Benjamin Reinheimer, Simon Stockhardt, and Ralf Tenberg

Technische Universität Darmstadt
Center for Advanced Security Research Darmstadt (CASED)
name.surname@cased.de

Abstract Phishing is 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 – be it in messages or in the address bar of the web browser. We developed a game-based smartphone app – *NoPhish* – to educate people in accessing, parsing and checking URLs; i.e. enabling them to distinguish between trustworthy and non-trustworthy messages and websites. Throughout several levels of the game information is provided and phishing detection is exercised in a playful manner. Several learning principles were applied and the interfaces and texts were developed in a user-centered design.

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 120.000 unique phishing attacks in the first half of 2014, i.e. more than 120.000 impersonated websites [2]. Furthermore, they report that the average up-time of phishing websites was 32 hours and 32 minutes. During this time potential victims have to be self-reliant, i.e. they have to check the URL in order to know whether the destination is trustworthy. People could be supported by tools such as the Netcraft Extension [3]. However, such tools can never provide 100% accuracy [4]. Therefore, the tools' checks need to be complemented by humans checking the URLs. Yet, many people lack the required knowledge to properly check URLs [5,6] and assess the trustworthiness of a given website. Some people are even not aware of faked messages and websites at all and, thus, are not aware that they should check URLs before providing sensitive information [7,5].

Several solutions have been proposed to address the problem of lacking knowledge e.g. tutorials or guides [8,9], quizzes [10,11] and games [4,12]. Tutorials are read-intensive if they cover all the different channels (such as email, SMS, QR codes, instant messaging, and social media) and URL spoofing tricks phishers exploit. The quizzes we are aware of do – if at all – indirectly educate people based on the feedback whether given answers are correct or incorrect; i.e. they

do not explain why answers are correct/incorrect. In addition, they do not cover all different channels and tricks phishers exploit. The game Anti-Phishing Phyllis [12] only focuses on the email channel. Anti-Phishing Phil 1 and 2 [4,13] 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.

Our goal[1] 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 – be it in messages or in the address bar of the web browser. We opted for an Android smartphone app since in particular smartphone users are much more likely to access phishing websites than desktop users [14]. The detection of phishing on mobile browsers is complicated because in many cases address bars disappear and even if shown only parts of the URL are visible. Furthermore, a smartphone app provides the opportunity of casual gameplay and thus, compared to desktop solutions, more flexibility and time-independence. Thanks to the Google Play Game Services it is also possible for users to compare their performance with others. This adds a supplementary challenge and a motivational aspect, both key characteristics of gameplay and therefore successful learning. Furthermore, *NoPhish* integrates a number of learning principles recommended by literature.

2 Preliminary Considerations

2.1 Required Skills

Earlier phishing attacks could be detected by checking messages and websites for spelling and grammar mistakes or for design flaws. But since phishing attacks get more advanced, the URL is the only reliable indicator for the authenticity and trustworthiness of messages and websites (note, assuming a non-compromised system). Correspondingly, the following skills are required to successfully protect against phishing:

- Being aware that messages, links and websites can be easily impersonated;
- Knowing that the URL is a reliable indicator for the authenticity and trustworthiness of a website rather than a website's content;
- Knowing how to access and view entire URL;
- Knowing how to parse the URL properly;
- Knowing different URL spoofing tricks;
- Knowing the importance of HTTPS when entering sensitive data.

2.2 Target Group

With *NoPhish*, we address in particular people who lack knowledge regarding all the aspects listed in Section 2.1; but people who use the Internet frequently.

[1] Note, a summary of this paper is availalbe at [31]

We assume that *NoPhish* users have a general interest in learning to protect themselves (as they decided to install the app). Furthermore, our target group are Germans[2].

2.3 Learning Focus

URLs can either be checked using the URL preview function (cf. Figure 1) provided by several email clients and mobile browsers or directly in the mobile browser's address bar. We decided to educate people how to check URLs in the address bar for the following reasons: First, not all applications provide such a preview function, e.g. Android's (e.g. version 4.2) standard email client (e.g. version 4.4.2) does not provide such a preview function. Second, well-crafted URLs can still deceive users since the preview URLs are cropped in case they are too long (cf. Figure 1). We are aware that this decision comes with the disadvantage that users might fall for an attack by clicking on a link already, e.g. they could download malicious software. This issue is addressed by *NoPhish* in the final remarks (cf. Section 3.5).

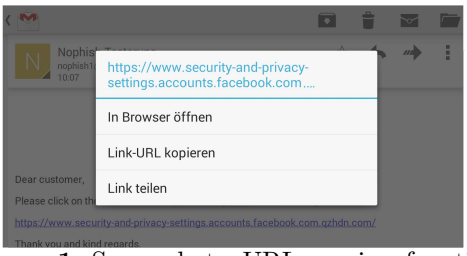


Figure 1: Screenshot - URL preview function

2.4 Categorization of URL Spoofing Tricks

Phishers apply several URL spoofing tricks. Different tricks should be explained in different levels of *NoPhish*. There are several approaches to categorize URL spoofing tricks [4,6,15]. We propose to use a different categorization; one that is based on the difficulty to detect the corresponding spoofing trick. Such a categorization is most appropriate for the later leveling. Correspondingly, we identified the following categories (note, the examples are taken from PhishTank):

a) *IP Address URL without Brand:* Sometimes phishers do not even bother registering any domain at all. In this spoofing trick, the host area of the URL contains an IP address while the path part does not contain the brand name, e.g. http://5.178.64.164/secure to impersonate PayPal.

[2] Note, this has an impact on the language as well as on the selected URLs and the design of the app.

b) *Random/Unrelated/Trustworthy Domain, without Brand:* This trick uses random/unrelated or trustworthy names or strings as domain name[3] and does not include the brand name of the targeted website in any other part of the URL. E.g. http://www.szuhsa.fr/login.html, http://www.weather.com/login.html or https://secure-payment.com to impersonate PayPal.
c) *Random/Unrelated/Trustworthy Domain, with Brand in Subdomain:* A phisher can include the brand name into the subdomain of a URL in combination with a random/unrelated/trustworthy domain name, e.g. http://paypal.mark-chippy.com/account-setup/ or http://www.amazon.account.com/.
d) *Random/Unrelated/Trustworthy/IP Domain, with Brand in Path:* A phisher can include the brand name into the path part of a URL in combination with a random/unrelated/trustworthy domain name, e.g. http://online-payment.com/www.paypal.com/. This attack can also happen in combination with an IP address URL, e.g. http://5.178.64.164/paypal.
e) *Derivated Domains:* A phisher can register a modification of the original domain. In this case the modified domain contains the brand name in some form, e.g. facebook-login.com can be registered in order to impersonate facebook.com.
f) *Introducing Typos:* Phishers can register domains which resemble the targeted domain, but have a typo, e.g. the phisher can register micosoft.com to impersonte microsoft.com. One special case of the typo is swapping letters in the original domain name, e.g. mircosoft.com to impersonate microsoft.com.
g) *Replacing Character(s):* A phisher can also exploit character resemblance, i.e. the phisher can register domains where characters are replaced by other similar characters, e.g. https://www.arnazon.com.

There are some more URL spoofing tricks which either cannot be recognized by the human eye (e.g. homograph attacks [16]) or are irrelevant for our setting because they are redirected URLs such as tiny URLs [17] or cloaked URLs [18]. After succefully completing the last level of the game, some general remarks on these issues are provided to the users (cf. Section 3.5).

2.5 Learning Principles

This section explains the principles of learning according to [19,20] which are essential for increased learning performance:

Readiness: The principle of readiness states that motivation is crucial for effective learning. Note, due to the definition of the target group we assume that *NoPhish* users entail readiness.

Exercise: The principle of exercise is composed of two aspects: First, training and repetition help increase learning. Second, feedback is crucial for good learning performance. Ideally, these two aspects are applied in combination.

[3] Note, that we refer to the first- and second-level domain of a URL as domain.

Effect: The principle of effect states that people who associate their learning with positive feelings, e.g. early successes, learn more and better while on the other hand, negative feelings can decrease the learning performance. Correspondingly, enabling early success and maintaining people's motivation with positive feedback is crucial for successful learning.

Intensity: The principle of intensity states that learning is encouraged by things that are more intense. E.g. people are likely to learn more from an exciting and enthusiastic teacher than from a boring and monotone one or from a text book.

Primacy: The principle of primacy states that the first thing people learn makes the strongest impression; i.e. it should be started with important content.

2.6 Gamification

The following game elements are used in most modern games [21,22] and are important for a good game experience:

Lives: An inherent element of a game is the possibility of losing it. If users are not able to lose a game they have no incentive to win it or play it. At the same time, one does not want the user 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.

Levels: Leveling serves multiple purposes: First, it is important for the users to get a feeling for the progress they make. Second, it provides fixed points in the game from where they can restart or pause and continue the game later on. Finally, it enables to increase the difficulty of the game with increasing levels.

Achievements: Achievements are special elements of a game that users can unlock if they, e.g. find a special object or if they play a certain level exceptionally well. This is in particular for people who are 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.

Leaderboards: A leaderboard is an area where a user can compare the own progress in the game with the one of other users. The comparison with others motivates people to improve skills relevant for the game resulting in better performance.

2.7 User-Centered Design

The design and implementation of a user friendly and understandable app as described by Abras et al. [23] is achieved by giving extensive attention to the users' needs and wants as early as possible.

3 Game Design

This section elaborates on the game design and explains how the identified aspects of Section 2 are addressed.

3.1 Initial Survey

Before elaborating on the app design and implementation we inteded to get an idea of the users' preferences with regard to an anti-phishing education app. Thus, we ran an initial user survey where we asked users whether they would prefer a rather neutral game or a comic style education game with e.g. a fish as main character. The results of our survey confirmed previous findings by Volkamer et al. [24] that for a German audience (adults at least) a rather neutral game-based approach would be best accepted.

3.2 Learning Content per Part

The app entails two introductory parts, the game with nine levels, and a final remarks part. Table 1 shows the link between the skills to properly judge on the trustworthiness of websites (cf. Section 2.1) and the different parts of *NoPhish*.

Taught Skill	**Covered in**
Awareness of fake messages, links and websites	Intro Part 1
Access and view entire URL	Intro Part 2
URL as a reliable indicator for phishing attacks	Intro Part 2
Proper URL parsing	Level 1
Different URL spoofing tricks (cf. Section 2.4)	Levels 2-8
a) IP address, no brand	Level 2
b) Random/unrelated/trustworthy domain, no brand	Level 3
c) Random/unrelated/trustworthy domain, brand in subdomain	Level 4
d) Random/unrelated/trustworthy/IP domain, brand in path	Level 5
e) Derivated domains	Level 6
f) Introducing typos	Level 7
g) Replacing character(s)	Level 8
HTTPS for entering sensitive data	Level 9

Table 1: Skills – Levels – Assignment

3.3 Introduction Parts

After a short introduction to the problem of phishing and its consequences, *NoPhish* starts with two introductory parts. The *awareness of spoofed messages, links, and websites* can be best addressed by actually sending corresponding messages and *access and view entire URL* can be best exercised in the mobile browser. Thus, these two parts are seperated from the actual levels of the game.

Part 1 - Awareness of Spoofed Messages, Links, and Websites: First, users are made aware of how simple it is to spoof messages, e.g. emails [25]. 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 received email contains information that this email was sent by *NoPhish* and that users should check the "from field" to notice that this is actually the email they prepared. Furthermore, the email contains a link with the displayed text "https://www.google.de/" and users are asked to follow the link. Clicking on this link redirects the users back to the app. Thereby, users learn by experience that they should not trust displayed link texts. Back in the app some further information is provided, e.g. that website spoofing is simple as well. Finally, the user is informed that this kind of forgery is not only possible with emails, but also with other forms of communication, such as social networks, SMS or instant messaging systems.

Part 2 - Access Address Bar and View Entire URL: This part teaches the users how to access and view the entire URL in the mobile browser. In detail, the users are told (1) that they need to scroll up the entire website to make the generally hidden address bar reappear; and (2) that they need to tap the text field of the address bar and scroll to the left in order to view the entire URL. The explanations how to do so are supported with corresponding screenshots.

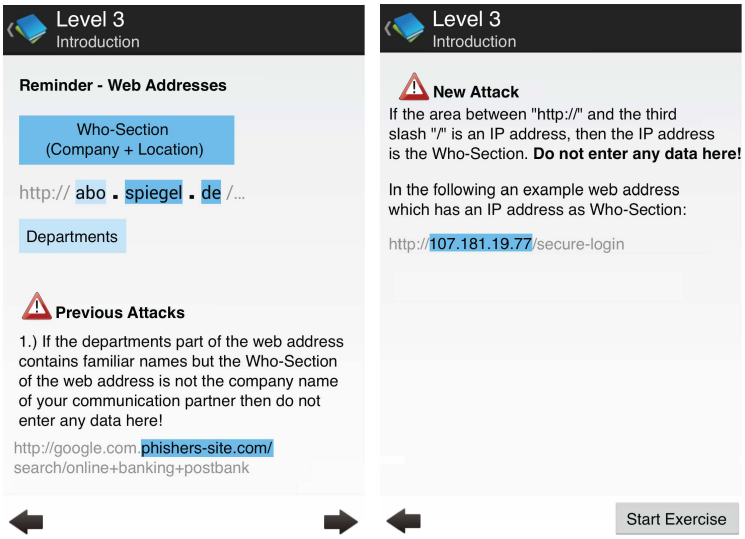
Due to the learning principle of *exercise* (cf. Section 2.5) after the explanations an exercise follows. Here, users are required to access the URL of a website they are forwarded to by *NoPhish*. Note, forwarding happens in a way that users first have to scroll up. On top of the page, there is a text 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. At the end of the exercise the users are told that URLs are the only reliable indicator for phishing. They also learn that they should always access the URL just as learned and that all other displayed links might be spoofed (by referring to the previous part). This part closes by explaining that URLs need to be carefully checked and that they learn how to do so throughout the coming parts of the app.

3.4 Gaming Part

The gaming part is split into nine 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[4],

[4] Note, this reminder is not shown if the user immediately starts off the new level after having successfully completed the last one but only if some time passed since the user played previous levels.

which provides a summary of previous levels (cf. Figure 2(a)) and the introduction of a new URL spoofing trick (cf. Figure 2(b)).



(a) Reminder (b) New URL spoofing trick

Figure 2: Example introductory block

The exercise is designed in a playful manner, 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. If the given answer is correct the users are rewarded by gaining points and a smiley face. This is relevant for the increase of positive feelings (cf. learning principle of *effect* in Section 2.5). If the answer is wrong the users lose points and a life. The users 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.

By practicing the learnt content and providing direct feedback we address the principle of *exercise* (cf. Section 2.5). Note, by making use of *levels* and *lives* two of the four gamification elements are already addressed (cf. Section 2.6). The elements *achievements* and *leadersboards* are realized by means of Google Play Game Services. Finally, *NoPhish* by nature provides intensity (cf. learning principle of *intensity* in Section 2.5) as it is a game.

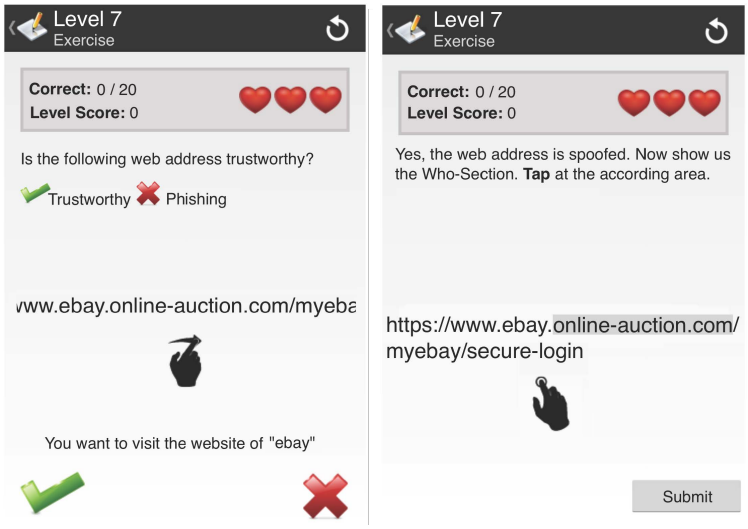
Level 1 - Structure of a URL: It is essential for people to achieve the capability of parsing a URL properly before learning different URL spoofng tricks. Especially the identification of the domain (first- and second-level domain) in a given URL is a key aspect which needs to be covered extensively. 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, the various URL spoofing tricks (cf. Section 2.4) are addressed. In level 2, we also explain IP addresses by using the analogy of house addresses (with street names and numbers).

During the exercises, URLs together with the name of the website the users are supposed to visit are displayed (cf. Figure 3(a)). Users are asked to decide whether they are legitimate or phishing ones. 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. This way, we prevent users from deciding based on the protocol.

When the users correctly identify a phishing URL, *NoPhish* asks them to tap on the *Who-Section* (cf. Figure 3(b)). This way, we aspire to ensure that they understood where to look at and did not just guess the answer. Depending on the



(a) Exercise - Phish/No Phish (b) Exercise - Show Who-Section

Figure 3: Example Exercise Screenshots

user performance the frequency of asking to tap on the *Who-Section* decreases or increases.

Note, in level n the number of URLs that need to be properly judged is $6 + 2 * (n + 1)$. The learning principle of *repetition* (cf. Section 2.5) is applied as each URL spoofing trick introduced in level n is tested in the exercises of later levels, too. About half of the phishing URLs (more precisely $\lfloor (6 + 2 * (n + 1))/4 \rfloor$

in level n) are repetitions[5] from previous levels. The first level that contains repetitions is level 3 because level 2 introduces the first URL spoofing trick.

Level 9 - HTTPS: In this level, we introduce the difference between HTTP and HTTPS. We explain, that HTTPS represents the higher security level and that this means (1) that the conversation cannot be eavesdropped by someone having access to the network and (2) that the communication partner indicated in the *Who-Section* proved his/her identity to a trusted authority if no warning is shown in the browser.

Furthermore, we tell users that there exist many legitimate websites without HTTPS (by default). We advice to try to switch to HTTPS. We explain the consequences if sensitive information is entered on a website without HTTPS (while assuming that the domain name is authentic). This level also includes an exercise. However, the question is changed. The users are asked whether they would provide sensitive information on the website. Thus, the users need to check whether a URL provides HTTPS and whether the domain name of the URL is spoofed or not.

3.5 Final Remarks Part

When the users reach the final remarks part they are well prepared for the detection of phishing URLs (cf. Section 2.1). Yet, there are some special cases the users are made aware of in this part of *NoPhish*. E.g. users are informed about further potential URL spoofing tricks that have not been exercised (redirected URLs and 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. In such a case, *NoPhish* suggests to directly contact the company and ask for the authenticity of the specific website, i.e. URL, before entering any data. Finally, *NoPhish* briefly introduces extended validation certificates and provides users with a link to further information on this topic. This part does not include an exercise.

4 App Development Process

This section gives a brief overview of our approach for the development of a user friendly and understandable app and summarizes the two most important steps regarding the development process – URL generation and user-centered design.

4.1 URL Generation

We generate phishing URLs by applying corresponding URL spoofing tricks to legitimate URLs. For the legitimate URLs 30 of the top 100 Alexa ranked domains (for Germany) were collected. The corresponding URLs have no path

[5] Repetition means that the URL spoofing trick is repeated not the specific URLs.

or subdomain, e.g. google.com. In order to also provide *NoPhish* users with longer URLs, we visited each of these websites, navigated through them and additionally picked three URLs for each domain, two long and one short URL. Thus, for each domain, a total of four URLs was added to the set of legitimate URLs. This set contains URLs with and without HTTPS.

For each URL to be displayed it is randomly decided which of the legitimate URLs is used. Then, it is randomly decided whether to show a legitimate or a phishing one based on the setting for the corresponding level. For the phishing URLs the corresponding URL spoofing trick is applied.

4.2 Applied User-Centered Design Approaches

In addition to the initial survey, we involved potential users of *NoPhish* in the following ways: we iteratively built, tested, and improved mock ups (while focusing on the first three levels as the app flow does not significantly change from this level on). For instance, according to comments of participants, we simplified and clarified the descriptions on how to access the address bar. We also reduced the text per page in general. The texts for all levels were reviewed by two German language experts (who are no security experts).

The next step was a user study, where we decided to go for the low cost method of guerilla user testing [26]; i.e. participants reading the app texts while thinking aloud. We included a little exercise in order to assess whether the users comprehended the texts or not, i.e. for each introduced URL spoofing trick we included a small list of URLs on which the users had to decide whether they were phishing URLs or not. Finally, the users were asked to provide their general impression. The received feedback was integrated.

In addition, we applied a statistical method – once we improved the text – in order to assess the legibility of our texts. Corresponding tools [27,28,29] take a regular text as their input and return a legibility index as their output. The average index value of the three tools for the entire text used in the app is 62. 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 [30]. Regarding our target group, this result is reasonable. However, it is something we have in mind for later user tests to evaluate.

5 Related Work

Section 1 already gives an overview of related work in anti-phishing education. Here, we especially elaborate on Anti-Phishing Phil 1 and 2 [4,13], as these games resemble *NoPhish* the most of all the anti-phishing education approaches.

Anti-Phishing Phil 2 uses a diver as main character (while Anti-Phishing Phil 1 uses a fish). A major improvement compared to Anti-Phishing Phil 1 is that the game emphasizes the importance of the domain. E.g. the users are asked to mark the part of a URL which indicates phishing. This is an aspect we

included to *NoPhish*. Furthermore, the information texts are generally improved and extended to be more precise.

The design of Anti-Phishing Phil 2 as such could not be applied for our context due to the results of our initial survey. However, we carefully analyzed the structure and the educated content to decide what could be adapted and what we wanted to modify or improve: The provided information, is often not precise enough and sometimes even inconsistent. In one information text the host is introduced as the part between "http://" and the first "/" and the domain is right before the first "/". In another information text the domain is addressed by referring to the right hand side of the host area, which could be either only the top level domain or could also include subdomains. In addition, Anti-Phishing Phil 2 covers only four URL spoofing tricks (similar to Anti-Phishing Phil 1): subdomain tricks, IP addresses, domains with hyphens (part of derivated domain names) and replacing character(s).

The users are asked to decide on only three URLs per level which seems not to be enough in order to internalize the learnt content according to the principle of *exercise*. Also, URL spoofing tricks from previous levels are not repeated which is essential for good learning performance according to the learning principle of *exercise*. Finally, the difference between HTTP and HTTPS is not addressed as well as the contents of introduction parts 1 and 2 of *NoPhish*.

6 Conclusion and Future Work

In the scope of this work, we have designed and implemented an anti-phishing education app – *NoPhish* – in a user-centered design approach. In a playful manner, users obtain valuable information on how to detect phishing URLs, in particular on a smartphone. The detection of phishing URLs is realized as a game, where the user can win or lose points or lives.

We integrated learning principles and diverse gamification elements recommended in literature. In order to provide levels, with increasing difficulty to detect phishing URLs, we proposed a new categorization of URL spoofing tricks which we then explain in the different levels.

The app is divided into two main parts: the security awareness and the educational part. In the security awareness part the user is shown how simple it is to spoof emails and links by sending themselves a spoofed email with a spoofed link. In the educational part the user is taught how to access the URL and how to detect phishing URLs.

We already conducted a user study including a retention study which showed very promising results [31]. In future, we also plan to assess how such an education app can best be distributed. An idea would be to utilize embedded learning [32] where simulated phishing emails are sent to users. Whenever users fall for such an email they could be proposed to download the education app. We also plan to extend the target group and consider kids and youth.

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 1h2014. Anti-Phishing Working Group (APWG), Lexington, MA
3. Netcraft: Netcraft extension. `http://toolbar.netcraft.com/` Accessed: 2014-06-05.
4. 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: Proceedings of the 3rd Symposium on Usable Privacy and Security. SOUPS '07, New York, NY, USA, ACM (2007) 88–99
5. Dhamija, R., Tygar, J.D., Hearst, M.: Why phishing works. In: Proceedings of the SIGCHI conference on Human Factors in computing systems, ACM (2006) 581–590
6. Lin, E., Greenberg, S., Trotter, E., Ma, D., Aycock, J.: Does domain highlighting help people identify phishing sites? In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM (2011) 2075–2084
7. Li, T., Han, F., Ding, S., Chen, Z.: Larx: Large-scale anti-phishing by retrospective data-exploring based on a cloud computing platform. In: Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on, IEEE (2011) 1–5
8. Bundesamt für Sicherheit in der Informationstechnik: Phishing: Gefährliche umleitung für ihre passwörter. `https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/phishing_node.html` Accessed: 2014-05-26.
9. OnGuardOnline.gov: Phishing. `http://www.onguardonline.gov/phishing` Accessed: 2014-05-26.
10. Online, S.S.: Race to stay safe. `https://www.staysecureonline.com/staying-safe-online/` Accessed: 2014-05-26.
11. SonicWALL: Sonicwall phishing iq test. `http://www.sonicwall.com/furl/phishing` Accessed: 2014-05-26.
12. Wombat Security Technologies: Anti-phishing phyllis. `http://www.wombatsecurity.com/antiphishingphyllis` Accessed: 2014-05-26.
13. Aleven, V., Chan, S.H., Moore, A., Sung, A.: Anti-phishing phil v2.0. `http://jackieweber.net/Projects/phil.html` Accessed: 2014-06-05.
14. Canova, G., Volkamer, M., Bergmann, C., Borza, R.: Nophish: An anti-phishing education app. In: 10th International Workshop on Security and Trust Management in conjunction with ESORICS 2014. Volume 8743 of Lecture Notes in Computer Science., Springer International Publishing (September 2014) 188–192
15. Boodaei, M.: 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: 2014-05-28.
16. Garera, S., Provos, N., Chew, M., Rubin, A.D.: A framework for detection and measurement of phishing attacks. In: Proceedings of the 2007 ACM workshop on Recurring malcode, ACM (2007) 1–8
17. Gabrilovich, E., Gontmakher, A.: The homograph attack. Commun. ACM **45**(2) (February 2002) 128–
18. Larkin, E.: Spot the tiny phishing trick. `http://www.pcworld.com/article/161232/tinyphish.html` (2009) Accessed: 2014-05-26.

19. Alnajim, A.: Fighting internet fraud: anti-phishing effectiveness for phishing websites detection. PhD thesis, Durham University (2009)
20. Thorndike, E.L.: The fundamentals of learning. Teachers College Bureau of Publications (1932)
21. Murphy, C.: Why games work and the science of learning. In: Interservice, Interagency Training, Simulations, and Education Conference. (2011)
22. Badgeville: Game mechanics. http://badgeville.com/wiki/Game_Mechanics Accessed: 2014-06-10.
23. Siering, G.: Gamification: Using game-like elements to motivate and engage students. citl.indiana.edu/news/newsStories/dir-mar2012.php (2012) Accessed: 2014-06-10.
24. Abras, C., Maloney-krichmar, D., Preece, J.: User-centered design. In: In Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications, Publications (2004)
25. Volkamer, M., Stockhardt, S., Bartsch, S., Kauer, M.: Adopting the cmu/apwg anti-phishing landing page idea for germany. In: Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on, IEEE (2013) 46–52
26. Avoine, G., Junod, P., Oechslin, P.: Computer system security: Basic concepts and solved exercises. EPFL Press (2004)
27. Simon, D.P.: The art of guerilla usability testing. http://www.uxbooth.com/articles/the-art-of-guerilla-usability-testing/ (2013) Accessed: 2014-05-26.
28. Stilversprechend: Stilversprechend. http://stilversprechend.de/index.html Accessed: 2014-05-26.
29. Leicht Lesbar: Testen sie ihren text. http://leichtlesbar.ch/html/ Accessed: 2014-05-26.
30. Schöll, P.: Flesch-index berechnen. http://www.fleschindex.de Accessed: 2014-05-26.
31. Amstad, T.: Wie verständlich sind unsere Zeitungen? Abhandlung: Philosophische Fakultät I. Zürich. 1977. Studenten-Schreib-Service (1978)
32. 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