Why Phishing Works on Smartphones: A Preliminary Study

Joakim Loxdal, Måns Andersson, Simon Hacks, and Robert Lagerström
School of Electrical Engineering and Computer Science
KTH Royal Institute of Technology
Stockholm, Sweden
{loxdal|manande|shacks|robertl}@kth.se

Abstract

Phishing is a form of fraud where an attacker attempts to acquire sensitive information from a target by posing as trustworthy. One strategy to fool the target is spoofing of a legitimate website. But why do people fall for phishing, and what security indicators are utilized or not utilized when deciding the legitimacy of a website? Hitherto, two studies have been conducted in 2006 and 2015. As time has passed since then, we like to check if people are meanwhile more certain in identifying spoofed websites. Therefore, 20 participants were observed when they analyzed and classified websites as legitimate or spoofed. On average participants had a success rate of 69 %, like previous studies results. The URL was used as an indicator by most of the participants (80 %), indicating user behavior and ease of identifying spoofed and legitimate websites is not very different on a smartphone compared to a desktop. Almost all participants used the content of the website at least once when deciding if a website was spoofed or legitimate. These findings will be used to conduct a bigger study to create more resilient results.

1. Introduction

Cybercrime is becoming more and more sophisticated and cyber criminals reached $ 3.5 billion in profits in 2019 [1], while phishing and extortion are the most common ways of scamming people. Phishing is a form of fraud where an attacker attempts to acquire sensitive information from a target by posing as a trustworthy entity [2]. The goal of phishing is often monetary gain by getting access to the targets information or access privileges [2].

Phishing is one of the largest security threats and contributes to 90 % of all data breaches [3]. In 2018, the Federal Bureau of Investigation estimated losses of $ 12 billion for companies worldwide due to phishing [4]. Commonly, attacker spoof a website and send a link to the target insisting that an action is required. On the website the target is asked to enter credentials that are monetized or allow access to sensitive information [5].

According to the Anti Phishing Working Group, the number of phishing websites in September 2019 were at the highest level since 2016 [6]. Hitherto, two studies have elaborated how spoofing websites fool users [7, 8]. However, since the last study five years have past and we plan to check if the findings of these studies are still eligible. In a first step, we like to determine the relevant aspects in a smaller study that will then be used in a second step for a broader study. Therefore, we examine what makes a phishing website convincing, and what methods users utilize to determine the legitimacy of a website when viewing it on a smartphone. This was examined through interviews where the participants were shown a random sample of websites (both legitimate and spoofed). The participants then decided if each of the websites were spoofed or legitimate. Previous studies have examined this in a desktop computer environment, but there is a lack of studies examining phishing susceptibility among smartphone users.

Our methodology is based on the methods used in the studies Why Phishing Works [7] and Why Phishing Still Works [8], but on smartphones instead of desktop computers. Smartphone phishing is a relevant subject to examine further since a majority of website traffic in 2019 came from mobile devices [9]. More concretely, we like to answer following research question in our work:

What are indicators that users utilize or fail to utilize to decide whether a website is legitimate or spoofed on a smartphone?

We expect that the URL (Uniform Resource Locator) is probably one of the most commonly used indicators when a user decides if a website is legit. Dhamija et al. [7] discovered that 77 % of the participants evaluated the address bar to make judgements on a websites legitimacy, 32 % used the padlock icon while only 9 % used certificates. Evaluating the sites overall design and functionality is probably the most common strategy (in

URI: https://hdl.handle.net/10125/71484
978-0-9981331-4-0

combination with other strategies), which was observed by both Dhamija et al. [7] and Alsharnouby et al. [8].

It is possible that more users will be able to correctly identify which websites are spoofed or legitimate on a smartphone than on desktop since there is less screen area to observe and examine. However, since less of the URL is visible in the browser window, it might also be more difficult. The fact that our study is performed on the participants own mobile devices might also make it easier to identify fraudulent websites, since some websites might open in apps and some might already be logged in.

The rest of this work is structured as follows: Next, we sketch related work. Especially, we explain two previous studies that elaborated on the same aspects as we. Afterwards, we explain our research method, before we illustrate the results of our study. Then, these results are discussed, and the threats of validity explained. Finally, we conclude our work and suggest future work.

2. Related Work

This study is based on the studies of Dhamija et al. [7] and Alsharnouby et al. [8]. These studies use a very similar methodology except for the fact that Alsharnouby et al. [8] utilize eye tracking technology to investigate where users look when they try to determine the legitimacy of a website. From the reports it can be concluded that studies were most likely performed in North America. The method used in both studies was that the users participating got to look at a collection of websites (24 and 19 websites respectively). For each website, the user was asked to decide whether they believed the website was legitimate or not.

The average success rate found by Alsharnouby et al. [8] for correctly identifying a website as either legitimate or not was 64 % compared to 58 % by Dhamija et al. [7]. However, considering the non-legitimate sites the success rate was 53 % and 54 % respectively. Even though 9 years passed between the studies, it does not seem like users are getting better at identifying fraudulent websites. For legitimate sites only the success rate was 79 % [8] and 75 % [7]. Drawing conclusions from comparisons of the studies should however be done with care since they used different websites for their studies even though the spoofing techniques used were similar. Additionally, the studies were limited to 22 and 21 participators respectively, meaning the results does not necessarily represent the average user.

Other related work is considering the transfer of the phishing concept to the mobile domain. Felt and Wagner [10] examine how vulnerable smartphones are to phishing. The study notes that security indicators are less visible for the user on smartphones, both when determining the identity of a website in a browser window and the identity of a running application, due to the limited screen size. Another risk factor on smartphones is that users often click on links in other applications (e.g., social media apps), which then display the website in an embedded browser window. The embedded browser window shows even less information about the website being visited, with smaller text.

Goel and Jain [11] bring up the fact that smartphones introduces new paths for phishing attacks. 87 % of all phishing attempts on smartphones are not carried out using email. Through text messages (SMS), MMS, and trusted mobile applications users are fooled to click links, get redirected, or share data. According to the article, mobile devices are three times more vulnerable to phishing attacks than desktop computers because of screen size, lack of awareness and inconvenience of user input. Therefore, separate techniques are needed to avoid these attacks.

Shahriar et al. [12] describe several mitigation techniques as suggestions against phishing on mobile devices. One technique is to analyze IP packets with machine learning. Another is to analyze if the layout of the visited website seems to be copying another websites layout. Another method to identify phishing websites is static analysis. The article mentions MobiFish, an anti-phishing application that detects IP URLs and warns the user. It also identifies forms on the website and warns the user if the website requests login-details. If it does, MobiFish searches for the host name in a whitelist. If the host name is not whitelisted and not displaying its domain name (excluding TLD) in the websites content, the user is presented with a warning. Other techniques about user authentication are discussed. The authors of the article suggest implementing several of these techniques to combat phishing.

3. Research Method

To answer our research question, we interviewed 20 users about their experience and reasoning while looking at legitimate and spoofed websites. We spoofed eight popular websites and their URLs using different techniques and provided nine legitimate websites. The participants were directed to a navigation site, which contained links to all the 17 web pages in random order.

The participants were recruited by sending out invitations on our respective Facebook accounts and to

Age	Sex	Phone Use/Day	OS	Browser	Tech. Prof.
25	M	4 h	Android	Chrome	4
22	M	3 h	Android	Chrome	2
57	F	6 h	iOS	Safari	2
22	M	5 h	iOS	Safari	2
57	F	2 h	iOS	Safari	0
50	F	2 h	iOS	Safari	2
20	F	5 h	iOS	Safari	3
29	F	2 h	iOS	Safari	2
56	M	3 h	iOS	Safari	4
22	F	4 h	iOS	Chrome	1
40	F	3 h	iOS	Safari	1
39	M	3 h	iOS	Safari	3
21	M	4 h	Android	Chrome	4
51	M	3 h	iOS	Safari	0
57	M	1 h	Android	Chrome	3
35	F	2 h	iOS	Safari	3
54	M	3 h	iOS	Safari	5
30	F	4 h	Android	Samsung Internet	2
56	M	5 h	iOS	Safari	2
68	F	1 h	iOS	Safari	0

Table 1. Demographic Information on Participants

two different Facebook groups. We also asked friends and family to recommend participants. Participants were rewarded with a movie ticket. We asked about the participants age, sex, and technical proficiency (on a scale from 0-5 as used by Alsharnouby et al. [8]) . We also asked about the participants smartphone operating system, browser as well as average time spent on their smartphone each day (actively), as illustrated in Table 1.

The users could use their own smartphone to make the study more realistic, and not have the UI of a different browser or operating system be a confusing factor. All interviews were conducted through the video conference app Zoom where participants shared their screen to make it easier for us to observe their behavior. For every website shown, we asked about the reasoning behind the participants decision and the difficulty they had to decide (on a scale 1-5). This is information gathered in previous similar studies and is therefore relevant when comparing our results.

To create the spoofed websites URL, we relied on five different techniques:

U1 A mistyped URL close to the original (e.g. ablidris.com instead of adlibris.com).

U2 A URL that is quite different from the original but might come off as legitimate (e.g. swedbank-privat.se instead of swedbank.se).

U3 A different top-level domain than the original (e.g. elgiganten.online instead of elgiganten.se).

U4 A sub domain used for deception (e.g. outlook.com-secure.live instead of outlook.live.com/owa).

U5 A URL consisting of a regular IP address (e.g. 35.228.129.249).

The websites were cloned using the tools HTTrack, wget, and the Firefox plugin SingleFile. For some clones manual tinkering was necessary in order to get the clone working properly. For example, there could be some JavaScript on the page that was not executing properly in the cloned version. Not all pages had all of their functionality cloned perfectly. However, this was not considered a problem, since it was found interesting to discover if users would be able to notice these flaws and raise suspicion.

To decide which websites to choose, we considered the top websites in Sweden using alexa.com and similarweb.com, as we wanted to ensure that most participants had visited the web page before. Our focus was on e-commerce (E), finance (F) and social media (SM) sites, since all those pages require login details. E-commerce and banking websites often require financial information, which motivates a phishing attack. In Table 2, we present all spoofed websites and in Table 3 all legitimate websites used in the study. We decided not to have for every legitimate website a spoofed website and vice versa, to avoid the possibility for the participant to deduct the status of a website due to its appearance before. Figure 1 illustrates ablidris.com (S5) on the left, and the legit adlibris.com (L6) on the right shown in Safari on iOS 13.

Before we performed the real study, we performed a pilot study on three volunteering PhD Students studying at our university. This pilot study was performed to test our methodology and receive feedback. The gained feedback resulted in an added progress indicator on the study website, a few fixed problems with the spoofed websites, and changing of the link styling so that visited links would not turn purple.

As the pilot study was finished, we started the real study. First, we gave a short introduction to phishing to each participant. We explained that phishing is often performed by creating a fake website mimicking a legitimate one to retrieve login or bank details from targets. Then, we presented the participant with a scenario inspired by the work of Dhamija et al. [7]: ”Imagine that you receive a message from a trusted person or company that asks you to click on one of the following links. Imagine that you decide to click on the

ID	Type	URL	Description	Method
S1	SM	https://fb.login.com.se	Facebook login	U4
S2	F	IP ADDRESS (http)	Klarna front page	U5
S3	SM	http://twitter.loginsecurity.online	Twitter login	U4
S4	E	https://ablidris.com/	Adlibris front page	U1
S5	F	https://swedbank-privat.se	Swedbank front page	U2
S6	F	https://skattesverket.se	Skatteverket front page	U1
S7	SM	https://outlook.com-secure.live	Outlook front page	U4
S8	E	https://elgiganten.online	Elgiganten front page	U3

Table 2. Spoofed Websites

ID	Type	URL	Description
L1	SM	https://outlook.live.com	Outlook front page
L2	F	https://internetbanken.privat.nordea.se/nsp/login	Nordea login page
L3	F	https://klarna.com	Klarna front page
L4	E	https://cdon.se	Cdon.com front page
L5	SM	https://i.reddit.com	Reddit mobile front page
L6	E	https://adlibris.com	Adlibris front page
L7	F	https://paypal.com	PayPal front page
L8	F	https://handelsbanken.se	Handelsbanken front page
L9	E	https://tradera.com	Tradera front page

Table 3. Legitimate Websites

link to see if it is a legitimate website or a fraudulent copy of that website."

Afterwards, the participants were directed to the navigation site of our study. It was explained to the user that the websites would be shown in a random order and that the same website could appear more than once. The latter was not true, as we included both spoofed and legitimate versions of some websites. If the user thought that a website would only appear once they might be able to use that information when the page appeared the second time. Finally, the participants were told to identify the websites as legitimate or spoofed. We stated that they could use the websites as any other website, but we emphasized that the first page they arrived at, was the one they were supposed to identify as legitimate or spoofed. This was clarified since our spoofed websites contained links to the legitimate version of each website.

4. Results

4.1. Demographics

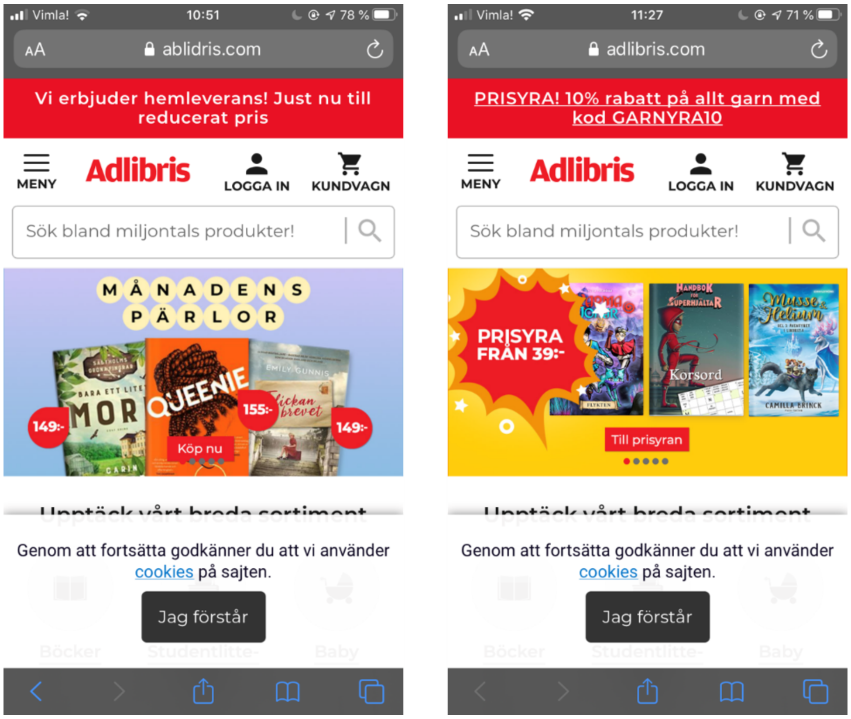
20 persons participated in the study, where 50 % were female and 50 % were male. 25 % used Android and the rest used iOS. The browser Safari was used by 70 %, followed by Chrome with 25 %, and Samsung Internet 5 %. Participants received 1 point for each correctly identified site and the total scores for each participant ranged from 7 to 17. The average number of points for all participants was 11.75 with a standard deviation (sd) of 3.04.

Furthermore, we calculated the correlation coefficient using Pearson Product-Moment Correlation [13] (N = 20) when comparing two sets of demographic characteristics. When comparing two populations t-test was used. A p-value < 0.05 was considered statistically significant for all tests. We could not discover a significant correlation between score and age (r = -0.243, p = .30), between score and technical proficiency (r = 0.408, p = .074), nor between score and active smartphone use per day (r = 0.382, p = .097).

However, we recognize a statistically significant correlation between score and sex. The mean score was 10.3 for females (sd = 2.39) and 13.9 for males (sd = 2.90). Lastly, we performed Levene's test [14] to ensure the homogeneity of the groups (F = 0.100, p = .755) and the t-test [15] (t(18) = 2.602, p = .018). The result shows that there is a difference between the male and female groups.

4.2. Recognition Rates

Following, we present the success rate of correctly identifying all our websites. The number shown in parentheses is the average confidence level (1-5) that participants reported for their correct/incorrect decision. Table 4 shows results of all the spoofed websites and Table 5 for the legitimate websites. The average number



Vi erbjuder hemleverans! Just nu till reducerat pris

PRISYRA! 10% rabatt på allt garn med kod GARNYRA10

Genom att fortsätta godkänner du att vi använder cookies på sajten.

Figure 1. Left the Spoofed Website and Right the Legitimate Website

ID	Correct	Incorrect
S1	90 % (3.5)	10 % (4.0)
S2	80 % (4.4)	20 % (4.5)
S3	65 % (3.5)	35 % (3.6)
S4	70 % (4.7)	30 % (3.8)
S5	50 % (3.7)	50 % (3.9)
S6	80 % (4.4)	20 % (4.5)
S7	60 % (2.7)	40 % (4.0)
S8	60 % (3.6)	40 % (3.9)
Total	69 % (3.7)	31 % (3.9)

Table 4. Results Spoofed Websites

ID	Correct	Incorrect
L1	75 % (3.7)	25 % (2.4)
L2	35 % (3.7)	65 % (3.0)
L3	65 % (3.5)	35 % (3.6)
L4	55 % (4.2)	45 % (3.3)
L5	50 % (3.2)	50 % (3.5)
L6	75 % (4.1)	25 % (2.6)
L7	80 % (3.6)	20 % (3.3)
L8	90 % (4.1)	10 % (4.0)
L9	95 % (4.0)	5 % (3.0)
Total	65 % (3.8)	35 % (3.2)

Table 5. Results Legitimate Websites

of correct guesses on all sites was 13.8 (69 % of the participants) and the median number of correct guesses was 14 (69 % of the participants). The standard deviation of number of correct guesses on all sites was 3.26.

4.3. Strategies

Several strategies and combinations of strategies were identified during the interviews. A participant was a user of a specific strategy if s/he mentioned something regarding the specific strategy at some point while evaluating the sites or if we observed the participant using the strategy. For example, if a user mentioned the padlock icon in the address bar at some point, s/he was considered using strategy 5 (”Using security indicators in the browser”).

Strategy 1: Evaluating the sites design Participants using this strategy considered the look and aesthetics of the website such as font, logos and layout. 90 % of the participants mentioned the sites design at least once in our study as a factor when deciding. Those who used this strategy at least once, had an average success rate of 68 % on all pages, compared to 76 % for the two participants that did not mention the sites design.

L2 Nordea and L5 Reddit are two examples where evaluating design lead to the wrong conclusion for legitimate sites. 25 % and 35 % respectively mistakenly classified the sites as spoofs with the design as motivation.

Strategy 2: Evaluating the sites functionality This strategy involves evaluating the sites behavior when interacting with different elements on the website such as links, buttons, forms and interactive animations. 95 % of our users evaluated the sites functionality at least once when trying to decide a sites legitimacy. This included participants clicking links on the site. Those using this strategy had an average success rate of 68 % compared to 82 % for the one participant who did not use this strategy at all.

An example of where this strategy was successful was when one participant noticed that the ”Visa Produkt” (show product) button did not work on the spoofed site S8 (Elgiganten) which helped him identify the site as spoofed.

Strategy 3: Evaluating the sites information Participants using Strategy 3 considered the information displayed on the website. This includes wording, spelling, type of information, and language. The difference from Strategy 1 is that this strategy considers what information is displayed instead of how it is displayed. 90 % of the participants used this strategy at least once during the interview. Those who used it had an average success rate of 70 %, compared to 74 % for the two participants who did not use it.

In some special cases users got a personalized version of a legitimate website. For example, one user was logged in to Outlook on their phone and the link to the legitimate Outlook front page redirected them to their inbox. The user used this as a basis for their decision that the website was legitimate. Some users also used the reverse argument, claiming that they should already be logged in on a specific site. Reddit opened in an app (instead of browser window) for 3 participants and Tradera for 4 participants.

The evaluating information-strategy had the most potential on the spoofed sites with outdated content. Only one user found outdated information and used it as a basis for labeling a website illegitimate. This was on S8 (Elgiganten), which described a weekly offer which was valid until a date that had already passed.

Strategy 4: Evaluating the sites URL A participant is considered a user of the strategy if they talked about the appearance of the URL at least once during the study. This strategy was used by 80 % of the participants. Participants using the strategy had an average success rate of 75 %, whereas participants not using it had a 44 % success rate. Some users were inconsistent and mentioned the URL at some point but did not mention it for most of the sites. Two users only mentioned the sites URL on one of the sites they evaluated. The maximum number of times the URL was mentioned was 16 which was done by two users. The average times mentioned (for those who utilized the strategy) was 9.2 (sd = 5.32). A statistically significant correlation was found between participant scores and number of times they mentioned a sites URL (r = 0.80, p = .000028).

On S1 (fb.login.com.se) 45 % of participants used the URL as motivation to correctly identify the site as spoofed. Even though the strategy was successful in general, it did not guarantee correct identification of spoofed websites. For example, one participant mentioned the URL of S5 (swedbank-privat.se) and still considered it legitimate. Two participants inspected or mentioned the URL of S7 (outlook.com-secure.live) but still classified it as legitimate. Some participants were suspicious about legitimate sites in Swedish having .com and not .se as TLD. For example, one participant incorrectly classified the legitimate klarna website (L3) as a spoof since it used .com instead of .se. On the legitimate site cdon.se (L4), the domain name was expected to be cdon.com by several participants.

The way the URL was displayed in the mobile browser window differed. One participant thought that the URL for S8 (Elgiganten) was giganten.online instead of elgiganten.online, since the address bar was cropped, caused by a smaller screen.

Strategy 5: Using security indicators in the browser This strategy involves looking at and interpreting the browsers security warnings and information displayed in the address bar, which differs along different browsers. The strategy was used at least once by 35 % of the participants. Those using it had an 80 % average success rate identifying all websites compared to 63 % average success rate for those who never used this strategy. One participant inspected certificates.

There were 5 legitimate sites (L2 Nordea, L4 CDON, L7 Paypal, L8 Handelsbanken and L9 Tradera) using EV-certificates. These sites had their host name and the padlock icon displayed in green in Safari, but not in Chrome or Samsung Internet. Only 14 % of participants using Safari mentioned the green padlock or green URL. One of those two participants mentioned the green URL on L2 (Nordea), but incorrectly classified the site as a spoof.

Strategy 6: Using a search engine to find the legitimate site One participant googled sites s/he was unsure about in a separate browser tab to determine if URLs and website content was identical. That participant had a success rate of 100 % on all sites, compared to the average of 67 % success rate for the other 19 participants.

Combinations of strategies All participants used a combination of at least three strategies. Participants who only relied on a combination of the website content-strategies (Strategy 1, 2 and 3), were the same group of people who did not utilize Strategy 4 (URL check). They had a low 44 % average success rate. The three worst performing participants in the study, with a success rate of 47 %, 47 % and 41 % respectively were all a part of this group.

Multiple participants showed that they did not understand that website content can be cloned quite easily. For example one participant said that ”It would be too exhausting to make a fake site like this” when mistakenly identifying S7 (outlook.com-secure.live) as legitimate.

Every participant who used strategy 5 (security indicators) also used strategy 4 (URL) and these participants had an average success rate of 80 %. Those who used strategy 4 but not strategy 5 had an average success rate of 71 %.

The three best performing participants all checked the URL (strategy 4) but only one of them mentioned security indicators (strategy 5). These three had a success rate of 100 %, 89 % and 89 % respectively.

5. Discussion

5.1. Spoofed websites

The three spoofing sites which fooled the largest number of participants used different URL spoofing techniques. Accordingly, there are no indications that one technique would be superior. However, they have in common that all three URLs contain the full name of the organization they are imposing as.

The spoofed sites that misspelled the organization name, S4 (ablidris.com) and S6 (skattesverket.se) fooled a relatively small portion of participants, 30 % and 20 % respectively. Maybe these sites would have been more successful in a real-world context, as we asked our participants to identify spoofed websites, which leads to a higher caution.

S2 (Klarna with IP address URL) and S1 (fb.login.com.se) were the spoofed sites that fooled the smallest amount of people. This indicates that the URL of a website is important for a user when deciding if a website is legitimate. Only one person thought the fake Facebook login site was legitimate even though the content of the site looked exactly like the real mobile Facebook login page. The usage of fb instead of facebook in the URL is probably a part of the explanation. The login.com.se domain name also felt suspicious for many participants.

The fact that the Klarna site (S2) with an IP address URL did not fool a lot of people is not surprising. The site also used http instead of https which meant that Safari displayed the text ”Not secure” to the left of the URL. Four people thought that the site was legitimate, none of those mentioned the IP address. It is noteworthy that this site fooled more people than the spoofed Facebook login site despite having an IP address URL. One explanation for that could be that the Facebook site (S1) was a login page, while the Klarna site (S2) was a front page.

5.2. Legitimate sites

The three legitimate sites that was hardest for our participants to identify correctly were L2 (Nordea), L5 (Reddit mobile) and L4 (CDON). This is not very surprising, since Reddit and Nordea use an old-looking design that many people mistakenly classified the sites as spoofs with the design as motivation. Nordea was not designed for mobile screens and had a long URL with two sub domains. Cdon.se had a success rate of just 55 % even though the URL was not suspicious, and they even had an EV-certificate. The reason for the low success rate was that many of the participants expected the domain for cdon.se to be cdon.com. Cdon.com was previously the brand name of cdon that was used in commercials and logos. Some participants also expected cdon to have a different product range.

Tradera (L9), Handelsbanken (L8) and Paypal (L7) were the easiest sites for participants to identify as legitimate. Tradera is a marketplace where people buy and sell almost anything. A reason that so many people identified it as legit may be that the site had a lot of content, displaying auctions with the time remaining. All the three sites have a clear URL containing only the organization name and a TLD which probably contributed to the legitimate impression. A modern design was also a common denominator for the three sites. Paypal had some flaws in the language used on the site. For example, there was an incomplete sentence that read ”Ta reda p varfr ver 255 miljoner.” (”Find out why over 255 million.”) Most participants (80 %) successfully identified the site as legitimate anyways.

An interesting find regarding security indicators was that most Safari users that could see the green URL and padlock in the address bar (representing EV-certificates) did not know how to use this information. This indicates that EV-certificates and indicators for it has not been understood by most users. This might be the reason for why most browsers does not indicate EV-certificates anymore. End users simply do not know how to interpret them.

The legitimate login page for Nordea (L2) was classified as a spoof by 65 % of participants while the spoofed Outlook page (S7) was identified as a spoof by 60 % of participants. This result indicates that the strategies used are not very effective and that a site with older looking design can be more suspicious looking than one with a spoofed domain name. Another possible reason for this could be that a login page made users more suspicious than a front page.

5.3. Participants strategies

It was noticed that almost all participants depended on a sites information, design, and functionality when deciding if it was legitimate or spoofed. This seems like an obvious thing to do when visiting a new site, but it is often not a successful strategy. This is indicated by the results where participants with a completely content-based strategy had a 44 % success rate compared to 75 % for those who mentioned the URL at least once.

Since there was always a 50 % chance to answer correctly some users applying only content-based strategies still got a decent result by discovering what they thought were errors in the spoofed websites design and information. For example, one user correctly identified S1 (fake Facebook login) as a spoof stating that the font in the Facebook logo was incorrect even though it was the real logo.

Looking at the security indicators and evaluating the URL proved to be a more successful than relying solely on the website content. 80 % of participants investigated the URL at some point and they had an average success rate of 75 %. One interesting find was that some users applied the URL-strategy once and then never used it again. A very significant and strong correlation was found between the success rate and the number of times a user mentioned the URL during the study. Furthermore, the users who not only mentioned the URL but also the browsers security indicators had an even better success rate at 77 %.

It is likely that the users that did not look at the URL had a bad understanding of how the web works. Therefore, it is a bit surprising that no significant correlation was found between technical proficiency and performance or between daily smartphone usage and performance. It is possible that the five questions that were asked to determine a participants technical proficiency were not accurate enough.

The only user with a 100 % successful strategy googled sites and compared them to the sites he was directed to in the interview. This is the most fool proof strategy identified and includes both URL and website content as factors. This strategy would also work when visiting a new site that you have not visited before, assuming it is a spoof and not a unique fraudulent website that the search engine has indexed. It is possible that other participants thought that they would not be allowed to use external sources to investigate the legitimacy of a website, but the instructions given did not limit the methods participants could use in any way.

5.4. Smartphone browser improvements

One of the main flaws made by participants when deciding if a spoofed website was legitimate or spoofed was to not look at the URL at all and focusing solely on content. Another flaw was misinterpreting the URL. This can be considered an error on the users side, but browsers can also affect how the users interpret the URL.

One way for browsers to make this easier for users could be to display the URL more visibly or even double check if the user really wants to move from one domain to another. This could of course be intrusive and make the browsing experience less comfortable.

A less intrusive approach could be to highlight the domain name somehow, like displaying it in a different color or higher opacity. This would make it easier to interpret the URL, as the domain name is the most important part of the URL when deciding a websites legitimacy. The host name outlook.com-secure.live (S7) in our study would perhaps not have been quite as effective if the domain name com-secure.live was highlighted. This is already done today in the desktop version of the browser Firefox. However, this might not help users not aware of what a domain name or URL is at all.

To expand on this idea, you could take it one step further and only show the domain name in the address bar. Currently Safari on iOS only show the host name but as was shown in the spoofed Outlook example, the host name can be deceptive. If only the domain name was shown the address bar for spoofed Outlook would have read com-secure.live instead of outlook.com-secure.live which probably would have raised suspicion among more participants. One could claim that it would be more difficult to know what website you are currently on if you could only see the domain name but it would still be possible to click the address bar and see the full URL at any time. This slight inconvenience could be worth it if there is a security benefit.

Another thing that makes it more difficult interpreting the domain name is that the address bar becomes hidden on Chrome when the user scrolls down on a webpage. The design choice makes sense since smartphones have less screen space and as much as possible is used for showing content. Safari on the other makes the address bar smaller when the user scrolls down on a page but never hides it completely. It is likely that this approach has significant security benefits, even we did not find such in our experiments.

5.5. Comparing with previous studies

The participants in this study had a better average success rate than the users in the works of Dhamija et al. [7] and Alsharnouby et al. [8]. The average success rate was 58 %, 64 % and 69 % by Dhamija et al. [7], Alsharnouby et al. [8], and this study respectively. For spoofed sites only the success rates were 54 %, 53 % and 69 %. For legitimate sites only the rates were 75 %, 79 % and 69 %. There could be numerous reasons for these differences, like different websites, different participants, or chance. An obvious difference between the studies was that we let participants use their own mobile devices. This led to the fact that some websites opened in mobile applications and that some were already logged in to a legitimate website. This was used by some participants to decide whether a website was spoofed or legitimate.

In previous studies, participants were considerably better at identifying legitimate websites correctly than spoofed websites. This was not the case in this study where the success rate was equal for both legit and spoofed websites. The participants in this study were more suspicious and more likely to consider websites fake overall. This could be due to cultural differences. Dhamija et al. [7] and Alsharnouby et al. [8] performed their studies in North America whereas this study was performed in Sweden.

6. Threats to Validity

The highest threat to validity in the study is that a couple of websites behaved differently on Safari and Chrome, and that all pages functionality was not cloned perfectly. The spoofed Klarna page (S2) had ”Download our app”-banner that only showed up on Safari. This was by their design and the same behavior was seen on the legitimate Klarna page (L3). The same difference was noticed on swedbank-privat.se (S5) after the study had been conducted, but in that case the same behavior was not seen on the legitimate site swedbank.se. This combined with many other variables makes it difficult to draw any conclusions about what URL spoofing technique was the most successful.

One other shortcoming of our study is that all participants were aware that the study was conducted and that their task was to identify legitimate and spoofed websites. This probably made the participants more careful and more observant. The results of the study indicate an upper bound of peoples ability to verify the legitimacy of a website.

The technical proficiency-questions in our interview might have been to arbitrary. They were slightly more focused on the web in general but perhaps they were not good enough to indicate the technical knowledge of a user. In future studies a different way to measure technical proficiency and a more precise definition of what is meant by technical proficiency would be beneficial. However, we decided to follow the approach of Alsharnouby et al. [8] to create comparability between our studies.

7. Conclusion

The results indicate that almost all ($>$ 90 %) of the participants evaluate a sites information, design and functionality when deciding if a site is legitimate or spoofed. This was not a successful strategy when used on its own, leading to a mere 44 % success rate for the few users who never mentioned the URL or security indicators. However, most participants (80 %) evaluated the URL of a website at least once during the interview. These people performed a lot better and had a 75 % success rate of classifying sites correctly. Those who not only mentioned the URL but also mentioned the browsers security indicators performed even better still with an 80 % success rate.

The results indicate that smartphone users are not more susceptible to phishing than computer users. About the share of participants evaluated the URL at least once during our study compared to previous studies made on desktop computers. No significant correlation was found between scores and age or active time spent on smartphone per day. This was also the case in the previous similar studies. Technical proficiency was not found to correlate with performance either. This is surprising since knowledge of how URLs and the web works in general seemed to be important during the interviews, but at the same time it matches previous studies results. More users correctly identified spoofed and legitimate websites in this study compared to previous studies. One reason is probably that our participants used their own devices and some websites opened in an app or were already logged in to their account.

Many users were confused about the meaning of padlock icon (HTTPS) and green text/padlock in Safari (EV-certificates). The domain name was sometimes hidden/partly hidden on participants smartphone screens, which could make identifying a spoofed website more difficult compared to a browser on a computer screen. Even when participants looked at the URL they were sometimes fooled by the spoofed websites. To combat this, browsers could display the URL in a clearer way. One suggestion is for browsers to only show the domain name in the address bar. This could help in the cases where the sub domain is deceptive.

Overall, the quantitative results of the study could show some indications when compared to the previous studies. We will take this indications to conduct a larger study in future to draw more definitive conclusions. With regards to user behavior it became clear that the participants that put too much emphasis on the website content performed very poorly in the study. Those who mentioned security indicators performed a lot better even though many of them did not fully understand their meaning.

Our study lacks a few perspectives that will be considered in our future study. Firstly, it lacks a big population which could lead to more conclusions. Secondly, it lacks a variety of spoofing techniques unrelated to the actual URL of the sites. One spoofing technique that would be interesting to test is the inception bar, a spoofed address bar suggested by James H. Fisher [16]. Thirdly, it might be of interest to research the influence of different aspects on the identification rate, like using different browsers, demographics, or security awareness.

Neither Dhamija et al. [7], Alsharnouby et al. [8], nor our results show a correlation between performance and technical proficiency. This is something we found surprising and it would be interesting to research this further. In that case, it would be wise to clearly define what technical proficiency means and try to find an accurate way of testing it. Further, it was previously mentioned that the reason for the difference in success rate when comparing with previous studies could be due to cultural differences, which can be of interest for future research as well. Future studies could focus on comparing different browser security indicators to make a more thorough analysis about which are more efficient.

Acknowledgment

This work has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement no. 832907, the Swedish Energy Agency, and the Swedish Governmental Agency for Innovation Systems (Vinnova).

References

[1] BBC, 2020 (accessed 2020-09-21). https://www.bbc.com/news/technology-51474109.

[2] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, no. 10, pp. 94–100, 2007.

[3] Verizon, "Data breach investigations report 2019," 2019.

[4] S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, "All about phishing exploring user research through a systematic literature review," in *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance*, University of Plymouth, 2019.

[5] A. Oest, Y. Safei, A. Doupe, G.-J. Ahn, B. Wardman, and G. Warner, "Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis," in *APWG Symposium on Electronic Crime Research (eCrime)*, (Piscataway, New Jersey), pp. 1–12, IEEE, 2018.

[6] APWG, "Phishing activity trends report 3rd quarter 2019."

[7] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (R. Grinter, ed.), ACM Digital Library, (New York, NY), p. 581, ACM, 2006.

[8] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *International Journal of Human-Computer Studies*, vol. 82, pp. 69–82, 2015.

[9] statcounter, 2020 (accessed 2020-09-21). https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet.

[10] A. P. Felt and D. Wagner, "Phishing on mobile devices," in *Web 2.0 Security and Privacy*, pp. 1–10, IEEE, 2011.

[11] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Computers & Security*, vol. 73, pp. 519–544, 2018.

[12] H. Shahriar, C. Zhang, S. Dunn, R. Bronte, A. Sahlan, and K. Tarmissi, "Mobile anti-phishing: Approaches and challenges," *Information Security Journal: A Global Perspective*, vol. 28, no. 6, pp. 178–193, 2019.

[13] K. Pearson, "Notes on regression and inheritance in the case of two parents," *Proceedings of the Royal Society of London*, vol. 58, pp. 240–242, 1895.

[14] M. B. Brown and A. B. Forsythe, "Robust tests for the equality of variances," *Journal of the American Statistical Association*, vol. 69, no. 346, pp. 364–367, 1974.

[15] E. L. Lehmann, "The probable error of a mean," *Biometrika*, vol. 6, no. 1, pp. 1–25, 1908.

[16] J. H. Fisher, 2019 (accessed 2020-09-21). https://jameshfisher.com/2019/04/27/the-inception-bar-a-new-phishing-method/.