Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector

Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector

Mattia Mossano
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany
mattia.mossano@kit.edu

Kami Vaniea
School of Informatics
University of Edinburgh
Edinburgh, United Kingdom
kvaniea@inf.ed.ac.uk

Lukas Aldag
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany
lukas.aldag@kit.edu

Reyhan Düzgün
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany
reyhan.duezguen@kit.edu

Peter Mayer
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany
peter.mayer@kit.edu

Melanie Volkamer
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany
melanie.volkamer@kit.edu

***Abstract*—Phishing is currently one of the biggest threats in cybersecurity for both the business and the private contexts. A large percentage of phishing attacks are blocked by automated technical solutions, but unfortunately there is often a delay between when phishing emails enter inboxes and when the technical solutions are able to detect and filter them out. To close this gap, it is common practice for companies to implement mandatory phishing awareness measures for their employees. But what about the private context? We aimed at answering that question by analysing 94 anti-phishing webpages from eight different countries and four organisation types. Our analysis revealed not only contradicting recommendations, but also that most of them are rather abstract (e.g. check the URL before clicking on the link without telling what to look for) and lack guidance on advanced phishing techniques (e.g. clone phishing). We discuss the problems faced by readers of these webpages and outline both immediate recommendations to the web designer and ways forward to improve the current situation as future work.**

***Index Terms*—phishing, user awareness, anti-phishing recommendations, anti-phishing material**

1. Introduction

Phishing is currently one of the biggest threats in cybersecurity to both organisations and private citizens [17]. According to Proofpoint, 88% of companies worldwide faced phishing attacks in 2019 [34]. Over the years, researchers have developed various technical solutions to detect phishing attempts, e.g. [2], [11], [36]. However, phishers are also improving their approach and using ever more advanced techniques resulting in phishing attempts that are not detected by technical solutions. This situation often leads to a time lag between when the phishing message is delivered to its recipient(s) and technical solutions being able to detect it as phishing.

To address this gap, companies implement security awareness measures to increase the likelihood that their staff will detect phishing messages - e.g. by explaining the phishing vectors (i.e. the delivery method) as well as popular tricks used by phishers. But what about those not working for a company that provides such measures? Prior work by Redmiles et al. shows that 67.5% of their respondents learned security behaviours from online, print, or TV news [40]. They also found that digital-service providers, such as banks, were a source of security recommendations for 33% of their respondents. These results suggest that people may be seeking out the recommendations found on large organisation webpages, in an effort to better protect themselves from various security threats, including phishing.

This observation leads to our research question: which anti-phishing recommendations can be found on the Internet, and are they helpful to readers? To answer the question, we collected 94 anti-phishing webpages from eight different countries and four organisation types. We used qualitative data analysis to identify the following aspects of interest: (a) webpage features, e.g. which type of visual support is used and which phishing vectors are presented, (b) phishing cues to look for, both in messages and website specific, (c) handling of detected phishes, and (d) action to be taken if the reader fall for a phish. We find that the anti-phishing webpages vary a lot in all these aspects. We also found contradicting recommendations - e.g. Caixa Bank [10]: “Spelling mistakes and other errors may alert you to a fake email or website,” vs. Police Nationale [33]: “Attention, the fraudulent messages are nowadays written in a perfect French. Orthographic mistakes do not allow anymore to identify or not a phishing attempt.” Furthermore, we noticed that most recommendations are rather abstract, e.g. check the URL before clicking on the link, without saying what to look for. They also lack advanced phishing techniques, e.g. clone phishing.

The conflicting recommendations and their variability could cause confusion or annoyance among readers of the webpages, leading to security fatigue [46]. The lack of advanced phishing techniques and the abstractness of the recommendations could also be the indirect cause

of various effects observed in other studies, such as reduced readers' self-efficacy [6], and low effectiveness with regard to increasing readers' ability to detect phishing attacks [35].

In the discussion we address the most prominent shortcomings we found, and we express some recommendations on how to solve them. Furthermore, we present our proposal for a lasting solution to the current situation and how we plan to achieve it.

2. Methodology

We first describe the process used to identify the organisations and their anti-phishing webpages. Afterwards, we present the qualitative analysis approach we adopted, i.e. how the codebook was created and applied.

2.1. Anti-phishing Webpages Collection Approach

For organisation types we chose the following four: Bank, Internet service provider (ISP), Governmental Agency, and University. These were selected as the most probable ones readers would consider visiting to obtain more information on phishing or in the event of a successful phishing attack.

Furthermore, we decided to restrict our study to webpages from the USA, Switzerland and the six most populous state members of the European Union (i.e. Germany, France, UK, Italy, Spain, and Poland). We decided to reduce the scope to only these countries both to obtain a more manageable amount of data and to avoid heavy reliance on automated translation. We consider three organisations for each of the four organisation types per country, i.e. 96 webpages in total ($96 = 3 \times 4 \times 8$, with 8 countries).

The selection of the first three organisation types (i.e. Bank, ISP, and University) was based on the data presented in corresponding lists: Standard & Poor's for the Bank type [44], [45], national market share reports for the ISP type [1], [7], [47]–[51], and QS World University Rating for the University type [39]. We proceeded top-down along each list until we found three organisations per type with an anti-phishing webpage.

For the remaining fourth organisation type (i.e. Governmental Agency), we selected the national consumer agency, the security agency, and the national government webpage of the respective country. We identified the respective webpages with web searches using the DuckDuckGo search engine [57] and the keywords "*country* consumers centre website", "*country* government website", and "*country* police website". Afterwards, we located the search tool on each one and use the keywords "antiphishing", "anti-phishing", "online fraud", and "fraudulent message" to locate the specific webpages providing recommendations on the subject. In case the anti-phishing webpage was not found using the English keywords, we used WordReference [22] to translate them in the appropriate language and run another set of searches using the search tool.

However, it was impossible to collect all the organisations for every country. Italy, Poland, and Spain have no information about phishing on their government webpage. To cope with the lower amount of webpages in the Governmental Agency type, we decided to increase their number by adding two EU[1] agencies and one extra UK webpage [15], [16], [18]. Also, only one Polish university provides an anti-phishing webpage.

The final selection of organisations contains therefore 94 organisations from 9 countries, instead of the expected 96 from 8 countries.

2.2. Qualitative Analysis

This subsection presents the method used to extract from the anti-phishing webpages the qualitative data to analyse and the how we proceeded in this analysis.

2.2.1. Data Collection. We employed NVivo 12 [37] for the open coding procedure to analyse the content of the selected anti-phishing webpages. NVivo 12 was selected as it is a software that allows the analysis of both language-based and visual-based qualitative data. Namely, the software allows to "Import text, audio, video, emails, images, spreadsheets, online surveys, web content and social media" [37] to be analysed. We captured every webpage with NCapture [38], a NVivo extension for Google Chrome and MS Internet Explorer. NCapture takes a screenshot in the NVivo file extension (.nvpx) of each webpage with all of its elements.

Note, cookie banners proved to be a problem for the software. Since the cookie banners are elements of the webpages, they were captured, often obscuring significant portions of the text. As the problem still persisted after accepting the cookies, we resolved the issue by installing another Google Chrome extension, called "I don't care about cookies" [23]. The extension explicitly accepts cookies and blocks the cookie banners from appearing[2].

2.2.2. Coding of the Material. To identify common and interesting aspects of the collected anti-phishing webpages, we started with an inductive coding approach [42], [53]. The aim of inductive coding is to identify frequent, dominant or significant aspects of text [53], in our case, what common aspects of the anti-phishing webpages exist that might impact the information a reader would learn from them. The lead researcher open coded three anti-phishing webpages from each of the four organisation types. This researcher then used the resulting codes to identify the most interesting aspects, resulting in 20 potential aspects. The potential aspects were then reviewed with other members of the research team who used group discussion to refine and narrow the aspects to those most interesting to study. Ultimately, eight anti-phishing webpage features and five recommendation aspects were selected to focus on. After scoping, the open codes were used to construct a hierarchical codebook where the top of the hierarchy were the 14 previously identified aspects, and the lower levels were codes pertaining to each of them. For example, the aspect *Visual example presence* have codes

1. While the EU is not a country, we explicitly decided to keep the organisation type name "countries", despite adding the EU agencies.

2. This behaviour was necessary for our research purpose, but it would be potentially harmful to readers' privacy. Therefore, we recommend against the use this extension.

below it of *No visual example* and *With visual example*. The coders then iterated on the design of the codebook by reading it, applying it on several anti-phishing webpages, and then discussing to further refine the codes and their definitions. The final codebook, with descriptions and examples, could be found in the supplemental material following the link https://secuso.aifb.kit.edu/anti-phishing-webpages-supplementals. Disagreements in coding were resolved through discussion. The coded material was then analysed with descriptive statistics.

3. Results

The results discussed in this section are shown in the tables 1, 2. Table 1 presents the results of the anti-phishing webpage features analysis. Table 2 presents the results of the analysis of the anti-phishing recommendations. The results for all aspects are provided in the tables. However, we want to use the following paragraphs to point out several particularly interesting findings.

3.1. Anti-Phishing Webpages Feature Analysis

This section presents the results of the webpages features analysis. The aspects presented describe both the structure of each anti-phishing webpage and the type of content presented. Namely, which phishing vector is described, the scope of the recommendations (if only about phishing, or on other cybersecurity threats), if there are visual examples, which types of examples, their origin, and if they highlight specific features, and if the webpage has a section to help phishing victims.

3.1.1. Overall. This section will present the results of all the anti-phishing webpage summed together, without distinction between organisation type nor country. Table 1 shows that the 94 anti-phishing webpages appear almost evenly split between recommendations on *Phishing by e -mail only* (45.74%) e.g. Société Général [20] and recommendations on *Multiple phishing vectors* (48.94%), e.g. Action Fraud [18]. Regarding the *Recommendations scope*, 58.51% of the webpages are limited to solely anti-phishing recommendations, e.g. Société Général [20], while 41.49% also consider other cybersecurity threats, e.g. Telecom (DE) [52].

Overall, almost 58% of the webpages provide only text information, and *No visual examples* of phishing messages, e.g. Comcast [12]. When there are visual examples, they are usually *Screenshots* of e-mails (67.39%), e.g. UCM [25]. Very few webpages employ videos (19.37%), e.g. MIT [29] or infographics (13.04%), e.g. Bank of America [28]. Among the visual examples, only 32% *Highlighted important features* that readers should considering when judging the legitimacy of a communication, e.g. Banco Santander [43].

43.62% of the anti-phishing webpages have an explanation section on what to do in case a reader becomes the victim of a successful phishing attack, e.g. BT [8]. 93.62% of organisations adopt a *Neutral tone* to communicate with readers, avoiding threatening language or friendly tone.

3.1.2. Organisation Type Specifics. Table 1 also presents the organisation type specific results. Looking at the phishing vectors presented on the organisation webpages, there are several differences between the types: Bank and Government Agency types usually have recommendations on *Multiple phishing vectors* (75.00%, 70.83%), while ISP and University webpages focus on *Phishing by e-mail only* (58.33%, 90.91%).

Regarding the *Recommendations scope*, we found an almost even distribution among organisation types, except for the University one, in which 86.36% pages offered only anti-phishing recommendations.

Considering the presence of visual examples, the data reveals that 50.00% of the Bank webpages show one, but this value decreases to 41.67% for University, and 37.50% for both Government Agency and ISP.

Regarding the presence of a section to help phishing victims, Bank and Government Agency type webpages are almost evenly split (50.00% and 45.83% with such a section). ISP and University types, instead, show a lower presence of such a section (37.50%, 40.91%).

3.1.3. Country Specifics. As can be seen in table 1, country results are usually evenly distributed; however, there are some interesting results worth noting. Regarding the recommendations scope, German and Polish webpages are almost evenly split between *Limited to phishing* and *On other cybersecurity threats* (50.00%, 40%). Visual examples are almost always screenshots, except for German webpages, where the number of videos and screenshots are the same (25.00%). Victim section presence is generally balanced, except for Switzerland (66.67% without) and Spain (where none of the anti-phishing webpages had such section).

3.2. Recommendations Analyses

Table 2 presents the results of the recommendation analysis. We will present the results divided by aspects: i) *Phishing cues*, describing what readers should look for to recognise a phishing attack. ii) *Web-site specific phishing cues*, which contains codes presenting the cues that readers should use to recognise a phishing web-page. iii) *Check directly when unsure*, recommending readers to contact a service directly, if they receive a mail that cannot identify as legit or malicious. iv) *How to react to phishes*, describing the action that readers should take to deal with phishing attacks once they recognise one. v) *What to do if fallen for a phish*, which describes the recommendations given to readers that are victims of a successful phishing attack.

3.2.1. Phishing Cues. Overall, we identify four recommendations as the most given ones in the Phishing Cues aspect, as shown in table 2. 70% of webpages inform readers that phishing attacks often *Ask for sensitive data*, e.g. “UPC Schweiz GmbH and other reputable companies will never ask you for your passwords or other personal information per email.” This very high frequency makes it by far the most given recommendation of the aspect, and the most given one among all other aspects.

All the webpages in the Bank type warn readers against communications requesting sensitive data, while

TABLE 1. OVERVIEW OF THE ANTI-PHISHING WEBPAGE FEATURE ANALYSIS. ORGANISATION TYPES: BA = BANK, GA = GOVERNMENTAL AGENCY, ISP = INTERNET SERVICE PROVIDER, UN = UNIVERSITY. COUNTRIES: EU = EUROPEAN UNION (INTERNATIONAL), FR = FRANCE, DE = GERMANY, IT = ITALY, PL = POLAND, ES = SPAIN, CH = SWITZERLAND, UK = UNITED KINGDOM, US = UNITED STATES OF AMERICA.

		Types				**Countries**								
Recommendations	All (%)	Ba	GA	ISP	Un	EU	FR	DE	IT	PL	ES	CH	UK	US
Phishing vector														
Multiple phishing vectors	46 (48.94)	18	17	9	2	2	4	4	5	6	5	7	7	6
Phishing by e-mail only	43 (45.74)	6	3	14	20	0	8	6	6	2	5	5	5	6
Non-specified phishing vector	5 (5.32)	0	4	1	0	0	0	2	0	1	1	0	1	0
Recommendations scope														
Limited to phishing	55 (58.51)	11	12	13	19	1	8	6	8	4	8	7	5	8
On other cybersecurity threats	39 (41.49)	12	13	11	3	1	4	6	3	5	4	5	8	3
Visual example presence														
No visual examples	54 (57.45)	12	15	15	12	0	6	8	8	7	5	6	9	5
With visual example	46 (48.94)	12	9	9	10	2	6	4	3	2	6	6	4	7
Visual example type														
Screenshot	31 (32.98)	8	5	9	9	1	5	3	2	2	6	5	1	6
Video	9 (9.57)	4	2	0	3	0	1	3	1	0	0	1	2	1
Infographic	6 (6.38)	1	3	1	1	1	1	0	0	0	1	0	1	2
Visual example origin														
From page owner	31 (32.98)	12	4	9	6	1	4	3	3	2	6	3	3	6
From other sources	11 (11.70)	1	5	0	5	1	3	1	0	0	1	3	1	1
Highlight important features														
No highlighted important features	25 (26.60)	20	23	20	16	2	10	10	9	9	9	9	12	9
With highlighted important features	15 (15.96)	4	1	4	6	0	2	2	2	0	2	3	1	3
Victim support section														
No section for victim support	53 (56.38)	12	13	15	13	1	5	7	6	5	11	8	5	5
With section for victim support	41 (43.62)	12	11	9	9	1	7	5	5	4	0	4	8	7
Tonality used														
Neutral tone	88 (93.62)	21	23	22	22	2	10	12	11	8	10	11	13	11
Alarming tone	3 (3.19)	2	1	0	0	0	1	0	0	1	0	1	0	0
Informal tone	3 (3.19)	1	0	2	0	0	1	0	0	0	1	0	0	1

among the other organisation types between 62.50% and 72.73% of anti-phishing webpages presented this recommendation to readers. When we look at the country results, we can see that Poland is the country with comparatively the fewest webpages that give this recommendation (44.44%).

The second most frequently given recommendation of the *Phishing Cue* aspect, with 45.74%, is watching out for *Poor grammar*, e.g. "Some frauds are easy to spot because they contain misspellings, misused words". Looking at the organisation type results, however, we can notice that Governmental Agency webpages present this recommendation less often than the others: 29.17%, against 58.33% for ISP type, 50.00% for Bank types, and 45.56% for University.

However, Government Agency type, alongside University, also inform readers that grammar has become better nowadays (respectively, 20.83% and 13.64%), e.g. "By the way, these emails are often perfectly formulated today, whereas at the beginning of the phishing attacks they were mostly written in very bad German." This is one of the cases of conflicting information we have identified.

40.43% of webpages tell readers that an *Unusual sender* address, is usually a phishing cue, e.g. "E-mail addresses used by scammers may differ from the authentic ones by easy to overlook details, e.g. typos in the domain name - instead of contact @ bank. pl - contact @ bank. ppl . Addresses may also contain a distorted or incomplete company or institution name."

Only 12.77% recommend readers to be wary of communications from *Unknown senders*, e.g. "Exercise caution and the principle of limited trust in messages from unknown senders."

The fourth most frequently given *Phishing cue* recommendation is to be wary of communications with an alarming tone trying to instil panic or threat (39.36%), e.g. "Be suspicious of any email with urgent requests for personal financial information."

However, when we explore the organisation type data, we can see that the ones giving this recommendation are mainly Bank and University types (58.33%, 50.00%); both the remaining organisation types only present it 25.00% of the time.

Lastly, 27.66% recommend against messages containing a link, and 23.40% webpages recommended to check the link destination before clicking, e.g. "They contain a link to a website". Only 12.77% recommend to check the attachment of a message, e.g. "BT will never send you an email with an attachment".

3.2.2. Website Specific Phishing Cues. The most given recommendation is *Check the URL in the address bar* (30.85%), e.g. "Also, look to see if the address in your browser's title bar is different to the one you expect." The organisation type that gives this recommendation the most is Universities (45.46%).

TABLE 2. OVERVIEW OF THE ANALYSIS OF THE ANTI-PHISHING WEBPAGE RECOMMENDATIONS. ORGANISATION TYPES: BA = BANK, GA = GOVERNMENTAL AGENCY, ISP = INTERNET SERVICE PROVIDER, UN = UNIVERSITY. COUNTRIES: EU = EUROPEAN UNION (INTERNATIONAL), FR = FRANCE, DE = GERMANY, IT = ITALY, PL = POLAND, ES = SPAIN, CH = SWITZERLAND, UK = UNITED KINGDOM, US = UNITED STATES OF AMERICA.

		Types				**Countries**								
Recommendations	All (%)	Ba	GA	ISP	Un	EU	FR	DE	IT	PL	ES	CH	UK	US
Phishing cues														
Ask for sensitive data	70 (74.47)	24	15	15	16	0	8	8	11	4	8	10	11	10
Poor Grammar	43 (45.74)	12	7	14	10	1	8	7	6	1	4	4	6	6
Unusual sender	38 (40.43)	12	5	10	11	1	5	6	5	3	3	5	4	6
Use alarming tone	37 (39.36)	14	6	6	11	0	6	3	3	1	4	7	7	6
Have a link to a website	26 (27.66)	6	1	1	1	0	0	0	2	2	2	0	3	0
Content account related	24 (25.53)	9	6	6	3	0	5	2	3	3	1	3	1	6
Content too good to be true	24 (25.53)	6	7	9	2	0	4	2	3	2	3	4	4	2
Generic greeting	23 (24.47)	7	5	8	7	1	3	5	3	0	2	2	4	3
Link destination	22 (23.40)	3	3	7	3	1	4	2	2	1	1	3	4	4
Unexpected communication	19 (20.21)	5	8	3	3	2	1	1	1	0	2	3	6	3
Have an attachment	12 (12.77)	4	0	6	2	0	0	4	0	2	1	2	2	1
Unknown sender	12 (12.77)	5	3	3	1	0	1	3	0	2	2	2	1	1
Bad layout	11 (11.70)	3	3	4	1	1	0	2	2	0	2	0	3	1
Content payment related	10 (10.64)	4	4	2	0	0	1	1	0	0	0	2	3	3
Content software related	7 (7.45)	4	1	2	0	0	2	1	1	2	0	0	1	0
Grammar better nowadays	5 (5.32)	0	2	0	3	0	1	1	1	0	0	1	0	1
Ask to not check with legit	2 (2.13)	1	1	0	0	0	0	0	0	0	0	0	1	1
Web-site specific phishing cues														
Check URL in address bar	29 (30.85)	7	7	5	10	1	3	2	6	2	3	3	3	6
Check for https	22 (23.40)	8	6	6	2	0	3	1	4	2	4	3	2	3
Type URL yourself	20 (21.28)	11	2	5	2	1	1	4	6	2	2	1	1	2
Check for lock icon	17 (18.09)	7	3	5	2	0	3	1	2	2	4	2	2	1
Bookmark sensitive websites	8 (8.51)	2	2	2	2	1	0	1	3	0	0	1	2	0
Check website legitimacy	4 (4.26)	1	1	2	0	0	1	0	0	0	0	2	0	1
Https not certain anymore	2 (2.13)	0	1	1	0	0	1	1	0	0	0	0	0	0
Do not bookmark websites	1 (1.06)	1	0	0	0	0	0	0	1	0	0	0	0	0
Lock icon not certain anymore	1 (1.06)	0	1	0	0	0	0	1	0	0	0	0	0	0
Check directly when unsure	52 (55.32)	14	12	12	14	2	7	4	7	3	5	6	12	6
How to react to phishes														
Don't click embedded links	57 (60.64)	16	18	12	11	2	7	9	8	4	2	8	10	7
Report attempt to page owner	40 (42.55)	16	5	8	11	0	5	5	5	4	2	2	9	8
Don't download or open attachment	39 (41.49)	14	10	10	5	1	6	5	3	3	5	7	5	4
Don't reply to the phish	32 (34.04)	8	9	6	9	1	6	3	4	3	4	2	5	4
Delete the phish	26 (27.66)	10	2	9	5	0	4	3	3	2	1	3	6	4
Report attempt to other organisation	24 (25.53)	5	12	5	2	1	5	0	1	2	1	3	5	6
Don't open the phish	7 (7.45)	1	3	2	1	0	2	1	2	0	1	0	1	0
Mark the phish as spam	1 (1.06)	0	0	1	0	0	0	1	0	0	0	0	0	0
What to do if fallen for a phish														
Change your password	21 (22.34)	2	5	7	7	0	5	2	3	0	2	1	5	3
Check account activity	15 (15.96)	5	4	5	1	0	1	1	5	0	0	3	3	2
Report theft page owner	15 (15.96)	9	1	0	5	0	2	2	3	1	0	2	2	3
Report theft financial institution	11 (11.70)	0	4	6	1	0	1	1	1	0	1	1	4	2
Block compromised accounts	9 (9.57)	4	4	1	0	0	2	2	2	0	0	1	1	1
Report theft dedicated agency	4 (4.26)	1	1	2	0	0	0	0	0	0	0	1	2	1

Https and lock icon are recommended to be safe anti-phishing cues, at 23.40% and 18.09% respectively, e.g. "A secure website will start with https:// in front of the address.", "Check that the website presents the padlock symbol or that of a non-broken key, in the lower half of the screen, indicating a safe website."

However, two of the anti-phishing webpages tell their readers that https is no longer a safe anti-phishing cue and one single webpage notes that the lock icon is not as effective as before to identify phishing webpages, e.g. "HTTPS does not guarantee the authenticity of a website," "The security certificate, recognizable by the lock icon in the status bar, is no longer a protection against phishing."

3.2.3. Check Directly When Unsure. 52.33% of webpages provide this recommendation, e.g. "Contact the relevant institution immediately if you notice anything irregular with your bank account or other online accounts." It is evenly prevalent among organisation types, although country-wise the United Kingdom greatly outpaced all the other countries with 92.31% of webpages giving this recommendation.

3.2.4. How to React to Phishes. As shown in table 2, 60.64% of the anti-phishing webpages recommend to readers to avoid clicking on links embedded in dubious messages, e.g. "Do not use the address or link received by e-mail or instant messenger to log in.". Among the organisation types, University is the one with the lowest frequency (50.00%), while the Spanish webpages show this recommendation comparatively less frequently than all others.

More than 40.00% of anti-phishing webpages ask readers to report phishing attempts to the webpages' respective owner, although the precise dynamic is different among the organisation types: Bank, ISP, and University types specifically ask the readers to send them phishes somehow related to them, e.g. "Tell us at once about spear phishing emails purporting to be from Deutsche Bank!". Government Agency webpages request every phish that impacts their citizens, because these agencies are usually national organisations. However, only 20.83% Government Agency webpages also request phishing attempts to be sent to them. The majority of the requests for phishing attempt reports are from Bank (66.67%) and University types (50.00%). Among the countries, UK, France, and USA are the ones that present this recommendation most frequently.

Conversely, Government Agency webpages are the ones that most likely recommend to report the attempt to a different organisation (50.00%), e.g. "Inform the bank from which apparently the e-mail is from."

Just over 40.00% of anti-phishing webpages also recommend to avoid downloading or opening attachments of emails identified as phishes, since they might be malware, e.g. "Do not open the attachment of any suspicious e-mail"

27.66% of the webpages recommend to delete the phish, e.g. "Delete the phishing emails". However, only one ISP webpage also recommends to mark the phishing message as spam, e.g. "Mark the e-mail as spam."

3.2.5. What to Do if Fallen for a Phish. As it can be seen in table 2 the most common recommendation given to phishing victims on anti-phishing webpages is to change their password (22.34%), e.g. "Immediately change any passwords you might have revealed", followed by both *Checking the account activity* and to *Report theft* to the organisation owning the anti-phishing webpage (15.96%), e.g. "Meanwhile, you should review your bank and credit card statements for any unusual transactions or withdrawals and notify the bank immediately if you suspect any discrepancies."

Considering the latter from the organisation type point of view, we can see this recommendation is given virtually only by the Bank and University type. Apart from this, however, no big differences can be identified in either the organisation types and the countries.

4. Discussion

Phishers use a wide variety of vectors to send phishing, including e-mails, text messages, messengers like WhatsApp, and posts in social media [54]. Not to mention less modern vectors such as phone calls, posters, flyers, and stickers – while URLs may be behind text, logos, buttons, or QR codes. While this range can be vast, most of the anti-phishing webpages we analysed focused only on e-mail vectors. While e-mail is historically a very common threat vector for companies, it is by no means the only source of such threats. In 2019 Verizon reported 18% of clicks on phishing links to be happening via mobile devices [54] showing that users are increasingly engaging with phishing on such devices. Thus, a worried citizen who is searching for information about phishing might therefore inaccurately conclude from the presented data that phishing is only an e-mail issue and incorrectly assume that tools like WhatsApp are safe, even though they are not [58].

Also 94% of malware seems to be delivered via e-mail attachments and 45% being hidden in a Microsoft Office document [54]. Therefore, attachments remain a serious source of compromise, yet only 12% of the analysed anti-phishing webpages mentioned e-mail attachments as potentially dangerous. This omission seems to be especially prevalent among the 22 University webpages with over 90% focusing on e-mail as phishing vector, but less than 10% discussing e-mail attachments.

Some webpages recommend to check the correctness of the sender address. However, sender addresses are fairly easy to spoof [19], [21], [32], allowing the attacker to impersonate any organisation they see as the most promising for their attack. It is also possible for a phisher to compromise the valid account of an individual or organisation, then use that account to send phishing to others. Both attacks are serious, since the recipient may not be aware that from addresses can be inaccurate. Note, while 40.43% of anti-phishing webpages urged the reader to look out for unusual or unexpected sender addresses, none warned readers about the potential of the addresses being spoofed or compromised themselves.

Many anti-phishing webpages also suggested that the reader should look at the content of the e-mail and use elements such as the grammar, layout, and tone to judge if the e-mail is from a valid company. However, this approach is known to have issues as phishers improve in their ability to write well crafted phishing e-mails, e.g. clone phishing. This is a type of attack where a legitimate e-mail is replicated in all of its parts, but with links and/or attachments modified to malicious ones [32] and the sender address is spoofed. Being a copy of a legitimate e-mail, the only errors that could be present, if any, are those that the original sender would have done. This makes it indistinguishable from the original when only considering aesthetic features such as grammar or layout. Furthermore, as e-mail is the only channel for many online services to their customers, they also use time pressure and the likes to get readers attention, e.g. an authentic bill needs to be payed.

URL checking is especially critical since simply visiting a phishing webpage can be enough to get compromised by a drive-by download or another exploit [13]. Verizon lists drive-by downloads as accounting for roughly 10% of malware attack vectors [54]. However, almost one third of the analysed anti-phishing webpages comprised at least one webpage-specific phishing cue that readers should look out for. While the page authors may simply be trying to provide readers with additional cues on how to spot phishing, readers may not interpret the information in that way. Instead they may inaccurately decide that visiting a webpage is a safe as long as they inspect the webpage for the listed cues before entering any sensitive data.

One of the most effective methods of determining if an e-mail is legitimate or not is looking at the embedded links and comparing the domain of the URLs to the one expected from the organisation supposedly sending the e-mail [5]. Unfortunately, users are currently not very skilled at doing such comparisons unaided [3], [5], [31], [56].

These results might be not too surprising, as information on how to check for the destination of a link before clicking it or how to check the domain of a webpage before entering sensitive data was missing completely from almost all of the analysed webpages. Note, when something related to links was present, it only considered e-mail links, avoiding explanations regarding mobile devices or link find online, e.g. as part of a social network post.

Only half of the analysed anti-phishing webpages showed visual examples; the remaining ones deliver their recommendations purely as text. However, various literature on effective learning [14], [24], shows that memorising and understanding information is supported by visual examples. Thereby, examples will be most effective when integrated properly. They should not be just listed as examples for past phishing e-mails without further explanations why these are phishes and what one can learn from these examples. Instead, as more than a quarter of the anti-phishing webpages does, they should be used to illustrate the mentioned phishing cues.

Our analysis reveals that less than 60% of the anti-phishing webpages have a section regarding victim support. This is a serious shortcoming, as readers of anti-phishing webpages might be on them searching for solutions to a successful attack. However, we acknowledge that the victim support aspect is more complex in the private context than in the business one, because of the different reader motivations. Another angle to consider is that in the private context, the question who to call if one has fallen victim to an attack arises as a general problem. Usually, if one becomes the victim of a criminal activity, they would call the police. However, the police in many countries only recently started building up cybercrime competences and, while responsible for the prosecution of cybercriminals, it might not be able to support victims in fixing the potential problems.

This situation in which readers are exposed to outdated or incomplete information is hazardous, because it can easily lead to ”security fatigue” [46]: readers feeling overwhelmed by the number of different or even conflicting recommendations they receive on the anti-phishing webpages, might reject the recommendations and decide on their own accord which ones to follow. This should be avoided if possible, because readers might misjudge the importance of certain recommendations and fall into the trap of either ignoring important recommendations or trusting in unreliable ones. In both instances, they might ultimately be exposed to unnecessary risk.

To avoid security fatigue, reduce the inconsistency of the recommendations given, and to ease both maintenance and update of webpages and recommendations themselves, we propose the creation of a unified template, to be proposed to a central agency such as ENISA or CISA.

Employing this template would provide standardised content throughout all the anti-phishing webpages, solving the inconsistency issue. It would also provide an easy to implement tool to web designers. Moreover, it would ease the maintenance burden: whenever the recommendations would need updating, the template can be modified accordingly. Web designers would then need to check if they are employing the newest version or not, without preoccupying about its content.

5. Related Works

There have been several studies focusing on recommendations. These can focus on different topics and are collected in various ways. In the following, we want to give an overview of this research.

Regarding *research focusing on anti-phishing recommendations*, Butler and Butler [9] focused on effectiveness of anti-phishing related information allocated by financial institutes, including banks. They used the construct of information quality (IQ) to rate the effectiveness. This study specifically focused on South Africa and they point out that the available information is insufficient. In comparison to our study, we collected anti-phishing recommendations from multiple organisations and countries.

Orunsol et al. [30] analysed the effectiveness of publicly available anti-phishing webpages of banks in Nigeria. They used a pre and post test to asses the ability to detect phish. Between those two tests, the participants had to choose from a set of bank webpages they are accustomed to. The authors discovered a low level of effectiveness when asking participants to judge various messages with varying phishing cues. While the conclusion is similar to our - the exact issues with the webpages were not studied by them. In comparison to our study, Orunsol et al. did not analyse the webpages on their own, but rather the ability of detecting phish before and after reading recommendations from such webpages.

Volkamer and Hilt [55] analysed the content of 83 German webpages from different institutes that provide anti-phishing information while taking a closed coding approach. It was checked which aspects of the phishing awareness measure presented in [27] are covered by other sources and which aspects are missing in this phishing awareness measure. They also found that most provided recommendations remain abstract and don’t provide clear instructions.

Alnajim and Munro [4] for example examined the effectiveness of the most common user tips on phishing webpages detection. They created a so-called effectiveness score, based on four different criteria: ”The tip prevents most common clues”, ”solo reliability”, ”the clue cannot be spoofed”, and ”The tip does not produce false positives or false negatives”. While this study tried to apply four different criteria on anti-phishing recommendations, we tried to focus on how these recommendations were collected to create an overview. Furthermore, this study is from 2008 which might not reflect the current situation.

Another topic paying great attention to recommendations and user awareness is *password security and management*. Murray and Malone [26] for example conducted a study to find the main characteristics of password recommendations. The recommendations were collected from 21 sources by internet searches, standard agencies and multinational companies. The peculiarity of their study is that their framework included the cost-benefit ratio of each recommendation. Besides that, Murray et al. studied password recommendations, our focus is on finding and categorising existing anti-phishing recommendations. Unfortunately, the process of identifying the recommendations is less systematic than our own approach and

therefore difficult to replicate. However, future lists of anti-phishing recommendations could be evaluated in a similar way.

Redmiles, et al. [41] analysed the readability of publicly available *general security recommendation*. They asked Amazon MT users to search for security recommendations themselves on the Internet and provide the paper authors with the corresponding webpages. We consider our approach in identifying the webpages to be easier to replicate. Also, while readability is important, we found a number of issues with the content of webpages we analysed. We agree that once the issues with the content are fixed, one should analyse their readability.

6. Conclusion

This paper tried to answer a double research question: which anti-phishing recommendations can be found on the Internet and are they helpful to readers?

To this end, we selected and analysed 94 anti-phishing webpages from four organisation types and eight countries. We employed inductive coding to collect the main interesting aspects of both, the common webpage features and the recommendations given. Then we used these aspects to create a hierarchical codebook where the top of the hierarchy were the 14 aspects themselves, and the lower levels were codes pertaining to each one. At last, we analysed the data regarding the webpages' features and the recommendations by organisation type, by country, and as a whole, using descriptive statistics to highlight any interesting findings.

We found that the overall quality of the analysed anti-phishing webpages is in need of improvement. The recommendations given are oftentimes limited in scope, frequently oblivious of phishing vectors other than e-mail, and insufficient to handle advanced (yet contemporary) phishing techniques. The recommendations on the webpages are also too abstract, lacking the details needed to be properly employed by the readers. Moreover, some of the anti-phishing webpages show contradictory recommendations, potentially heightening the frustration of the readers and leading to security fatigue.

We argue that this lack of consistent, up to date anti-phishing information might be one of the causes why so many people are not able to detect phishing effectively. To address the identified issues with the available information, we propose as way forward the creation of a standardised template to be adopted by all anti-phishing webpages.

We believe that developing such template would make it easier for organisations to create their own effective anti-phishing webpage and therefore ultimately benefit readers who are seeking information on phishing attacks for both prevention and mitigation purposes.

7. Acknowledgements

This work was supported by the German Federal Ministry of Education and Research (BMBF) in the Competence Center for Applied Security Technology (KASTEL).

The authors also acknowledge the valuable feedback given by the members of the TULiPS Research Group of the University of Edinburgh.

References

[1] AGCOM, "Relazione annuale sull'attività svolta e sui programmi di lavoro," Autorità per le Garanzie nelle Comunicazioni, Tech. Rep., Jun. 2019. [Online]. Available: https://www.agcom.it/documents/10179/15564025/Documento+generico+11-07-2019/7b6a8cdb-b6cc-45ac-b1b4-ef5a674df5b4?version=1.0

[2] G. Ahmed Ali, "Phishing Email: Could We Get Rid of It? A Review on Solutions to Combat Phishing Emails," in *Emerging Trends in Intelligent Computing and Informatics*, F. Saeed, F. Mohammed, and N. Gazem, Eds. Cham: Springer International Publishing, 2020, vol. 1073, pp. 849–856, series Title: Advances in Intelligent Systems and Computing. [Online]. Available: http://link.springer.com/10.1007/978-3-030-33582-3_80

[3] S. S. Albakry, K. Vaniea, and M. K. Wolters, "What is this url's destination? empirical evaluation of users' url reading," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI '20, Apr. 2020, p. 1–12. [Online]. Available: https://groups.inf.ed.ac.uk/tulips/papers/albakry2020.pdf

[4] A. Alnajim and M. Munro, "An evaluation of users' tips effectiveness for phishing websites detection," in *2008 Third International Conference on Digital Information Management*. IEEE, 2008, pp. 63–68.

[5] K. Althobaiti, G. Rummani, and K. Vaniea, "A review of human-and computer-facing url phishing features," in *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019, pp. 182–191. [Online]. Available: https://groups.inf.ed.ac.uk/tulips/papers/althobaiti2019.pdf

[6] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Computers in Human Behavior*, vol. 38, pp. 304–312, 2014.

[7] Arcep, "The state of the internet in France," Autorité de Régulation des Communications Électroniques et des Postes, Tech. Rep. 2019, Jun. 2019. [Online]. Available: https://en.arcep.fr/uploads/tx_gspublication/report-state-internet-2019-eng-270619.pdf

[8] BT, "What is a phishing scam? is the email i have received genuine?" 2019. [Online]. Available: https://bt.custhelp.com/app/answers/detail/a_id/9191/~/what-is-a-phishing-scam%3F-is-the-email-i-have-received-genuine%3F

[9] R. Butler and M. Butler, "Assessing the information quality of phishing-related content on financial institutions' websites," *Information & Computer Security*, vol. 26, no. 5, pp. 514–532, Jan. 2018. [Online]. Available: https://doi.org/10.1108/ICS-09-2017-0067

[10] Caixa Bank, "How to prevent phishing," 2019. [Online]. Available: https://www.caixabank.es/particular/seguridad/phishing_en.html#how_they_works_-_examples

[11] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems with Applications*, vol. 106, pp. 1–20, Sep. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417418302070

[12] Comcast, "Phishing 101," 2019. [Online]. Available: https://corporate.comcast.com/comcast-voices/phishing-101

[13] M. Cova, C. Kruegel, and G. Vigna, "Detection and analysis of drive-by-download attacks and malicious javascript code," in *Proceedings of the 19th international conference on World wide web*, 2010, pp. 281–290.

[14] A. Eitel, K. Scheiter, A. Schüler, M. Nyström, and K. Holmqvist, "How a picture facilitates the process of learning from text: Evidence for scaffolding," *Learning and Instruction*, vol. 28, pp. 48–63, 2013.

[15] ENISA, "Phishing/Spear phishing," 2019. [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing

[16] Europol, "Infographic: Fraud Scams Targeting Employees," 2019. [Online]. Available: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/infographic-fraud-scams-targeting-employees

[17] FBI, "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic," Mar. 2020. [Online]. Available: https://www.ic3.gov/media/2020/200320.aspx

[18] A. Fraud, "Protect yourself from fraud and cyber crime," 2019. [Online]. Available: https://www.actionfraud.police.uk/individual-protection

[19] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*. Greater Noida, India: IEEE, Apr. 2016, pp. 537–540. [Online]. Available: http://ieeexplore.ieee.org/document/7813778/

[20] S. Gênérale, "Quelle sont le techniques de fraude par e-mail le plus répandues aujourd'hui?" 2019. [Online]. Available: https://particuliers.societegenerale.fr/securite/dernieres-alertes#_%C3%80%20retenir

[21] H. Hu and G. Wang, "End-to-End Measurements of Email Spoofing Attacks," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD, USA: USENIX Association, Aug. 2018, pp. 1095–1112. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/hu

[22] M. Kellogg, "Wordreference.com," 1999. [Online]. Available: https://wordreference.com

[23] D. Kladnik, "I don't care about cookies," May 2020, library Catalog: chrome.google.com. [Online]. Available: https://chrome.google.com/webstore/detail/i-dont-care-about-cookies/fihnjjcciajhdojfnbdddfaoknhalnja

[24] L. Lin, R. K. Atkinson, W. C. Savenye, and B. C. Nelson, "Effects of visual cues and self-explanation prompts: empirical evidence in a multimedia environment," *Interactive Learning Environments*, vol. 24, no. 4, pp. 799–813, 2016.

[25] U. C. Madrid, "¿qué es un correo fraudulento?" 2019. [Online]. Available: https://www.ucm.es/faq/correo-para-tiucm/que-es-un-correo-fraudulento

[26] H. Murray and D. Malone, "Evaluating password advice," in *2017 28th Irish Signals and Systems Conference (ISSC)*. IEEE, 2017, pp. 1–6.

[27] S. Neumann, B. Reinheimer, and M. Volkamer, "Don't Be Deceived: The Message Might Be Fake," in *International Conference on Trust and Privacy in Digital Business*. Springer, Cham, 2017, pp. 199–214.

[28] B. of America, "How to avoid email phishing scams," 2019. [Online]. Available: https://bettermoneyhabits.bankofamerica.com/en/privacy-security/how-to-avoid-email-scams

[29] M. I. of Technology, "Learn how to avoid a phishing scam," 2019. [Online]. Available: https://ist.mit.edu/news/phishing_warning

[30] A. A. Orunsolu, A. S. Sodiya, A. T. Akinwale, B. I. Olajuwon, M. A. Alaran, O. O. Bamgboye, and O. A. Afolabi, "An Empirical Evaluation of Security tips in Phishing Prevention: A Case Study of Nigerian Banks," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 25–39, Mar. 2017.

[31] E. Pearson, C. L. Bethel, A. F. Jarosz, and M. E. Berman, ""To click or not to click is the question": Fraudulent URL identification accuracy in a community sample," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. Banff, AB: IEEE, Oct. 2017, pp. 659–664. [Online]. Available: http://ieeexplore.ieee.org/document/8122682/

[32] D. Pienta, J. B. Thatcher, and A. C. Johnston, "A Taxonomy of Phishing: Attack Types Spanning Economic, Temporal, Breadth, and Target Boundaries," in *WISP 2018 Proceedings*, vol. 1, 2018, p. 18. [Online]. Available: https://aisel.aisnet.org/wisp2018/19

[33] Police Nationale, "Le phishing (homeçonnage), gare aux faux sites!" 2019. [Online]. Available: https://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime/Prevention-contre-le-phishing

[34] Proofpoint, "2020 State of the Phish: An in-depth look at user awareness, vulnerability and resilience," Proofpoint, Inc., Tech. Rep., 2020. [Online]. Available: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf

[35] S. Purkait, "Phishing counter measures and their effectiveness–literature review," *Information Management & Computer Security*, 2012.

[36] I. Qabajeh, F. Thabtah, and F. Chiclana, "A recent review of conventional vs. automated cybersecurity anti-phishing techniques," *Computer Science Review*, vol. 29, pp. 44–55, Aug. 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1574013717302010

[37] QSR International, "Learn More About Data Analysis Software | NVivo," 2020. [Online]. Available: https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/about/nvivo

[38] ——, "NCapture," 2020. [Online]. Available: https://help-nv.qsrinternational.com/12/win/v12.1.90-d3ea61/Content/ncapture/ncapture.htm

[39] QUacquarelli Symonds Limited, "QS World University Ranking 2019," 2019. [Online]. Available: https://www.topuniversities.com/university-rankings/world-universityrankings/2019

[40] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How I learned to be secure: a census-representative survey of security advice sources and behavior," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 666–677.

[41] E. M. Redmiles, M. Morales, L. Maszkiewicz, R. Stevens, E. Liu, D. Kuchhal, and M. L. Mazurek, "First steps toward measuring the readability of security advice," 2018.

[42] J. Saldaña, *The coding manual for qualitative researchers*, 2nd ed. Los Angeles: SAGE, 2013, oCLC: ocn796279115.

[43] B. Santander, "Guía para protegerte contra el phishing," 2019. [Online]. Available: https://www.bancosantander.es/es/particulares/banca-online/seguridad-online/aprende-seguridad-online/phishing

[44] Standard & Poor Global, "Europe's 50 largest banks by assets," Apr. 2018. [Online]. Available: https://platform.mi.spglobal.com/web/client?auth=inherit{#}news/article?id=44033607&cdid=A-44033607-14380

[45] ——, "The world's 100 largest banks," Apr. 2018. [Online]. Available: https://platform.mi.spglobal.com/web/client?auth=inherit#news/article?id=44027195&cdid=A-44027195-11060

[46] B. Stanton, M. F. Theofanos, S. S. Prettyman, and S. Furman, "Security Fatigue," *IT Professional*, vol. 18, no. 5, pp. 26–32, Sep. 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7579112/

[47] Statista, "Poland: fixed-line internet providers 2018," Dec. 2018. [Online]. Available: https://www.statista.com/statistics/1008526/poland-fixe-line-internet-providers/

[48] ——, "UK market share of internet service providers 2019," Feb. 2018. [Online]. Available: https://www.statista.com/statistics/387678/uk-market-share-of-internet-service-providers/

[49] Statista, "Broadband connections: market share in Germany 2017," May 2019. [Online]. Available: https://www.statista.com/statistics/460237/broadband-connections-market-share-germany/

[50] Statista, "Internet usage by provider in Spain 2019," Apr. 2019. [Online]. Available: https://www.statista.com/forecasts/1001423/internet-usage-by-provider-in-spain

[51] ——, "World's largest telecom companies by revenue 2017," Apr. 2019. [Online]. Available: https://www.statista.com/statistics/221382/revenue-of-top-30-global-telecommunication-operators/

[52] Telecom, "Phishing: Gefälschte rechnungen per e-mail — telekom hilfe," 2019. [Online]. Available: https://www.telekom.de/hilfe/rechnung/rechnung-erhalten/echtheit-rechnung-per-e-mail?samChecked=true

[53] D. R. Thomas, "A General Inductive Approach for Analyzing Qualitative Evaluation Data," *American Journal of Evaluation*, vol. 27, no. 2, pp. 237–246, Jan. 2006. [Online]. Available: https://doi.org/10.1177/1098214005283748

[54] Verizon, "2019 Data Breach Investigations Report," Verizon, Tech. Rep., 2019. [Online]. Available: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[55] M. Volkamer and T. Hilt, “Sensibilisierung für phishing und andere betrügerische nachrichten,” *Datenschutz und Datensicherheit-DuD*, vol. 44, no. 2, pp. 121–125, 2020.

[56] M. Volkamer, K. Renaud, and P. Gerber, “Spot the phish by checking the pruned URL,” *Information and Computer Security*, vol. 24, no. 4, pp. 372–385, Oct. 2016. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2015-0032/full/html

[57] G. Weinberg, “Duckduckgo,” Sep. 2008. [Online]. Available: https://duckduckgo.com

[58] E. O. Yeboah-Boateng and P. M. Amanor, “Phishing, smishing & vishing: an assessment of threats against mobile devices,” *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 4, pp. 297–307, 2014.