SoK: Still Plenty of Phish in the Sea — A Taxonomy of User-Oriented Phishing Interventions and Avenues for Future Research

Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig, Christian Reuter, Alexander Benlian, and Joachim Vogt, *Technical University of Darmstadt*

https://www.usenix.org/conference/soups2021/presentation/franz

This paper is included in the Proceedings of the Seventeenth Symposium on Usable Privacy and Security.

August 9–10, 2021

978-1-939133-25-0

Open access to the Proceedings of the Seventeenth Symposium on Usable Privacy and Security is sponsored by

SoK: Still Plenty of Phish in the Sea — A Taxonomy of User-Oriented Phishing Interventions and Avenues for Future Research

Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig,
Christian Reuter, Alexander Benlian, Joachim Vogt
Technical University of Darmstadt

Abstract

Phishing is a prevalent cyber threat, targeting individuals and organizations alike. Previous approaches on anti-phishing measures have started to recognize the role of the user, who, at the center of the target, builds the last line of defense. However, user-oriented phishing interventions are fragmented across a diverse research landscape, which has not been systematized to date. This makes it challenging to gain an overview of the various approaches taken by prior works.

In this paper, we present a taxonomy of phishing interventions based on a systematic literature analysis. We shed light on the diversity of existing approaches by analyzing them with respect to the intervention type, the addressed phishing attack vector, the time at which the intervention takes place, and the required user interaction. Furthermore, we highlight shortcomings and challenges emerging from both our literature sample and prior meta-analyses, and discuss them in the light of current movements in the field of usable security. With this article, we hope to provide useful directions for future works on phishing interventions.

1 Introduction

Phishing is a frequently employed cyber attack to get hold of users' sensitive information, such as login details or banking account numbers. Furthermore, criminals increasingly use phishing attacks to distribute malware [90]. The consequences of a successful attack can reach from individual personal losses or compromised accounts to complete organizations or networks being infected by malware, often combined with ransom demands. For example, the years between 2014 and 2020 were marked by *Emotet*, a modular trojan using targeted phishing emails with weaponized Microsoft Word files [27, 58]. It is crucial to consider that phishing attacks do not primarily target hardware or software vulnerabilities, but the user – the human factor within the socio-technical system. While there are several tools and approaches that aim to identify malicious contents automatically (e.g., [78, 82]), the increasingly sophisticated and personalized nature of phishing attacks makes it hard for algorithms to detect and block phishing emails, websites, or malicious software. This leaves a large amount of responsibility to the user. However, detecting phishing attempts is not the user's first priority [93], for instance, while using email programs: Instead, users in various contexts aim to efficiently solve their tasks and answer what they perceive to be emails sent by customers or colleagues when they become victims of a phishing attack.

To enable users to be the ultimate wall of defense in cyber security, research and practice have developed a number of user-oriented interventions against phishing attacks. Among those are education and training approaches (e.g., [12, 44, 72]), where users develop knowledge and skills that they can transfer to real-world phishing attempts. To complement these, awareness-raising measures or design considerations (e.g., [25, 51, 56, 61]) aim to guide users towards secure online behavior in situ.

While developing adequate countermeasures that assist end-users in combating phishing attacks is highly relevant, finding both effective and usable user-oriented phishing interventions is still an unresolved problem [3]. Considering the diverse research landscape on phishing interventions across various research disciplines (e.g., cyber security, human-computer interaction, or social science), it is challenging to gain an overview of what types of interventions have already been investigated. The design of interventions may significantly differ between phishing attack vectors, the moment at which the intervention takes place, or approaches that increase the attention in a specific moment vs. those that encourage long-term capability to deal with phishing attacks autonomously.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

To our knowledge, a comprehensive literature review of existing approaches is missing to date. We argue that a systematization of prior phishing interventions, particularly with respect to their variety across multiple characteristics, will help to identify trends and gaps in the phishing intervention literature. Furthermore, a discussion in the light of current usable security movements will lead to a better understanding of promising directions for successful user assistance in the phishing context. Our research thus aims to shed light on the following two research questions:

RQ1: How does current research on user-oriented phishing interventions tackle the aim of guiding users towards secure online behavior?

RQ2: Which avenues for future research emerge from the existing phishing intervention literature?

In this work, we offer a comprehensive systematization of user-oriented phishing interventions with respect to the intervention type, the addressed attack vector, the moment at which the intervention takes place, as well as the degree of user interaction. We thereby complement broader reviews such as the work of Zhang-Kennedy & Chiasson [99], who have reviewed tools for cyber security awareness and education more generally. Our contributions are threefold: First, we present an extensive literature analysis of prior research on user-oriented phishing interventions [9, 69], bridging the research streams of both educational and design measures. Guided by previous rudiments of phishing intervention classifications [39, 43, 85, 94], we introduce a novel taxonomy of user-oriented phishing interventions consisting of four categories and ten subcategories. Second, we explore central characteristics such as the time at which the intervention takes place throughout the user's decision process, which phishing attack vectors are commonly addressed by the studied interventions, and the degree of user interaction required. Beyond that, we thirdly take into account critical considerations of leading usable security researchers (e.g., [20, 67, 84]) and discuss shortcomings of prior phishing intervention approaches. In summary, we offer a novel insight into phishing intervention research and present potential avenues for future works.

2 Methodology

To categorize and understand the landscape of existing phishing interventions, we have conducted a systematic literature review, following the "preferred reporting items for a systematic review and meta-analysis" (PRISMA) guideline [53, 55]. Literature reviews have been argued to play an important role in developing domain knowledge, e.g., by synthesizing prior research works, identifying research gaps, and developing a research agenda [69]. To cover the diverse research landscape, our initial search comprised the databases ACM Digital Library, IEEE Xplore, and Web of Science. The search was limited to peer-reviewed studies in English that were available as of June 2020.

The search term was identical across databases and applied to the title and abstract of all included articles. For an article to be included in the analysis, it had to contain the term *phish** and one of the following terms to allow for a plurality of intervention types: *interven** OR *prevent** OR *educat** OR *detect** OR *train** OR *nudg** OR *appeal*.

In addition to the database search, we analyzed the Google Scholar top ten security conferences and journals as well as the A* and A CORE-ranked security conferences and journals. Most of them had already been included in the analyzed databases (e.g., CHI, S&P, CCS, Computers & Security). Only journals and conferences that had not been covered by the previous database search underwent an additional manual title search. These included the USENIX Network and Distributed System Security Symposium NDSS and the accompanying usable security events USEC and EuroUSEC, as well as the USENIX Security Symposium and the co-located SOUPS conference from 2014 onwards[1]. In addition to our search term-based search, we have complemented our sample with two other relevant articles that we became aware of through our literature research.

With the above-described search procedure, we have identified a total of 2,124 publications. Afterward, we have conducted a title and abstract screening to exclude irrelevant articles. Articles were excluded if they matched one of the following criteria:

- Deals with a different topic not related to phishing in the sense of cyber security
- Intervention is not user-oriented in that the user cannot see or act upon an intervention (e.g., an algorithm that invisibly filters and blocks suspicious emails)

Table 1 in the appendix details the distribution across the different databases before and after the title and abstract screening. After the aforementioned procedure as well as the deletion of two duplicates, a total of 80 articles remained for a detailed analysis. As for the full-text screening, we have read and analyzed the 80 articles independently among the authors to ensure best possible thoroughness. Since this literature review has emerged from a cross-disciplinary collaboration between seven security researchers with backgrounds in computer science, information systems and psychology, we were able to discuss the literature from various angles and finally agreed on one final review. The full-text analysis further reduced the literature count by 16 articles: First, we excluded research works that did not address a user-oriented phishing intervention in the full text (see second exclusion criterion above). Second, we excluded similar articles by the same authors (e.g., a conference paper and a subsequent, very similar journal publication), and kept only the latest and more extensive version. Our final literature sample thus includes 64 articles.

[1] Before 2014, the SOUPS proceedings were included in the ACM database.

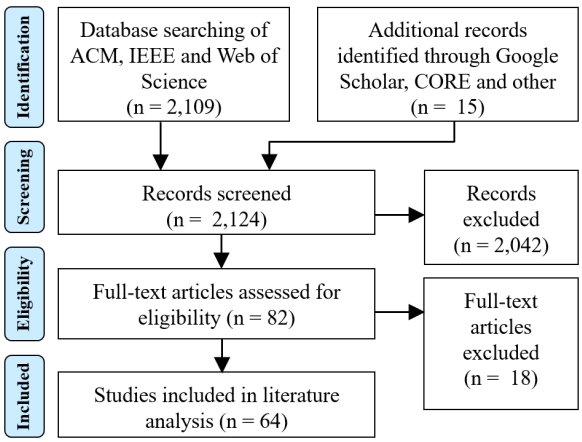


Figure 1: PRISMA diagram of literature screening process.

Figure 1 shows a flowchart that details the number of screened, excluded and included articles following the PRISMA statement [53, 55].

3 Results

In the following, we present a detailed analysis of our literature sample. We first provide an overview of the **methodological range** employed by previous phishing intervention research (Section 3.1). Categorizing the studied interventions with regard to their design and intended effect, we then derive a **taxonomy of user-oriented phishing interventions** (Section 3.2). We further consider the **phishing attack vector** that the intervention aims to address (Section 3.3), the **time at which the intervention takes place** (Section 3.4), as well as the **degree of user interaction** (Section 3.5).

For a comprehensive categorization of the analyzed phishing interventions across the whole literature sample, please refer to Table 2 in the appendix.

3.1 Overview of Methodological Approaches

With respect to the methodological approach, 13 research works have presented exclusively **conceptual ideas** of phishing interventions. For example, Dhamija & Tygar [24] have discussed factors that make securing users against phishing a challenging design problem and have derived design requirements for authentication schemes.

Studies that have gathered empirical data have drawn on **surveys** (3 publications), **lab** (20 publications), **online** (12 publications), or **field experiments** (16 publications) to analyze, e.g., the efficacy or usability of user-oriented phishing interventions. For instance, the effect of training material embedded in the process of sorting emails has been studied by Kumaraguru *et al.* [47], who have first employed a think-aloud vignette lab experiment, which has then been further tested in the field in the form of an online training game.

As for sample sizes, studies in our literature data range from small (< 20 participants) representative groups (e.g., [12, 36, 93]) to large-scale experiments with more than 1,000 participants (e.g., [47, 66, 85]). Field experiments were often conducted among university students and staff (e.g., [85]), rarely among non-university employees (e.g., [63]), or by evaluating real-world users' interactions with browser extensions or applications (e.g., [66]).

While most research articles in our sample have explored short-time effects of phishing interventions, some have employed longitudinal studies in order to investigate long-term effects. For example, Kumaraguru *et al.* [44] have observed knowledge retention of at least 28 days for users who had been trained via simulated phishing attacks and Silic & Lowry [73] have employed a long-term field experiment to investigate longitudinal effects of gamification on employees' intrinsic motivation to comply with security efforts.

With regard to the validity of experimental setups, previous works have pointed out that information security behavior research heavily relies on studying users' information security behavior as their primary activity on a computer [23,33,35]. In reality, however, responding to phishing threats is a secondary task that is embedded in a primary task, such as answering email or searching the internet. This leads to users facing the difficulty of switching between their primary and secondary activity, which may result in overlooking security warnings or disregarding educational offers. While many lab and online studies of our sample have studied their subjects' behavior as a primary task (e.g., by asking them to sort links into "legitimate" or "phishing" [5, 76]), others have assigned them fictional primary tasks to attend to. By using cover stories, such as sorting emails for a colleague or shopping online [43, 61], researchers have aimed to study phishing detection as a secondary task. However, it is arguable whether such artificial experimental setups can align with the complex nature of phishing. With regard to the realism of phishing experiments, Schechter *et al.* [68] have shown that role-playing participants behave less securely than those who act in a personal context (e.g., participants asked to log into a bank account with predefined passwords showed less secure behavior than those using their own passwords). While online or lab experiments are essential to test and refine theories of user behavior as well as to improve artifacts in human-computer interaction, conducting studies in a realistic environment is crucial to allow for robust and practice-oriented results. In our literature sample, less than one third (16 of 51) of experiments have been conducted in a real-world field setting.

3.2 A Taxonomy of User-Oriented Phishing Interventions

Our literature review has revealed that, while user-oriented phishing interventions all pursue one common goal (to protect users from phishing threats), they vary widely with regard

to their underlying concepts and intended effect. Prior literature has presented vague attempts of categorizations of phishing interventions. For example, Kirlappos & Sasse [43] have described two main approaches, namely anti-phishing indicators and user education, whereas Xiong *et al.* [94] have distinguished between warnings and training, and the integration of both. Similarly, Wash [85] has observed three styles of phishing interventions: general-purpose training messages that communicate "best practices", fake phishing campaigns, and in-the-moment warning messages. We chose to follow a fourth approach by Jansen & van Schaik [39], who have roughly described four different categories of user-oriented phishing interventions: **education**, **training**, **awareness-raising** and **design**. In their pure form, education and training interventions typically promote sustainable, long-term secure behavior, with the central aim that the application of knowledge and skills transfers to the real-world and enables users to engage in secure practices [79], whereas awareness-raising and design interventions aim to improve users' security during specific activities (such as logging into a website or reading an email) in the short term. Our literature analysis has revealed, however, that interventions often incorporate elements of more than one type.

Based on the literature data, we have derived a taxonomy of user-oriented phishing interventions as presented in Figure 2. In the following sections, we will describe the four categories and their respective subcategories in detail.

3.2.1 Education

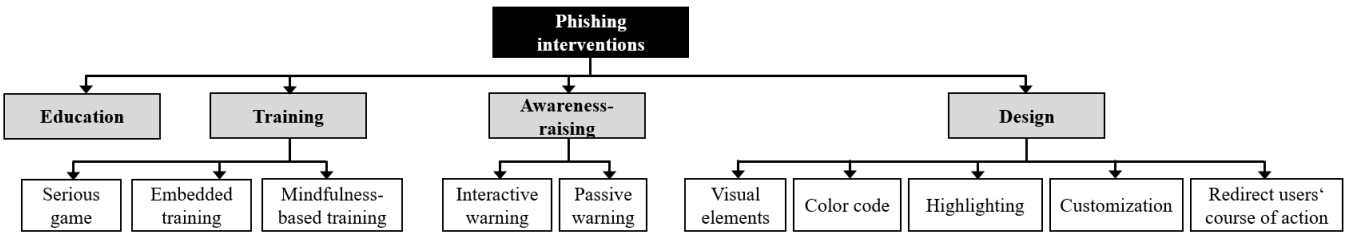
Purely educational interventions focus on developing knowledge and understanding of phishing threats and ways to mitigate them, e.g., by providing educational media, such as texts or videos, or by discussing online threats during in-class training. For this category, we have identified 7 publications in total. However, only three of them have considered education as a solitary intervention. For example, Wash & Cooper [85] have investigated which role the perceived origin of phishing education material plays in terms of effectiveness and have found that facts-and-advice-based training from perceived security experts surpasses the same training from peers. Four research works have studied phishing education in interaction with awareness-raising interventions by adding educational texts to fear appeals [39, 70] or warnings [95]. For example, Yang *et al.* [95] have found that a warning trigger combined with an educational text enhances its effectivity, whereas the educational element itself was not sufficient to provide phishing protection. Others have first provided extensive education in order to refer back to it during awareness-raising interventions later on [8]. Education interventions have been studied in rather traditional text-based, video-based or in-class formats. More progressive formats, such as online games, comprised interactive and hands-on exercises and were hence categorized as training.

3.2.2 Training

Compared with educational interventions, training goes one step further. It typically involves some kind of hands-on practice, where users develop skills that they can apply in case of a real threat. Since the term "training" is quite widespread in everyday language use, interventions that have been described as training by the respective authors might have been categorized as education within this work. Training approaches aim to enable users to identify phishing websites, phishing emails, or other malicious attacks. They employ interactive elements or exercises, where users can develop skills such as reading a URL, analyzing an email, or recognizing social engineering attempts. They often do so by exposing the user to a similar attack within a secure environment, either in an artificial or a real-world setup. Within our phishing literature data, about half of the publications (31 research papers) were dedicated to training interventions. Among them, we were able to distinguish several approaches.

Training interventions are typically rule-based. That is, their goal is to train individuals to identify certain cues to take protective action [76]. In our sample, 16 publications have explored such training in a **serious game** context, mostly taking place online and often focusing on teaching users how to identify phishing links by using cues in URLs (e.g., [5, 12, 72, 76]). For instance, Sheng *et al.* [72] have introduced "Anti-Phishing Phil", a game that is designed to teach users how to identify fraudulent websites based on the use of IP addresses, subdomains or deceptive domains in a URL. Similarly, "NoPhish" is a mobile app that guides users through several levels of analyzing and recognizing phishing URLs [12, 76]. The authors have found a long-term effect with regard to users' knowledge retention; that is, users who had played the NoPhish game have shown a better ability to decide upon the legitimacy of a URL. Silic & Lowry [73] have observed that gamified security training systems, which include elements such as levels or leader boards, enhance users' intrinsic motivation and yield better security behavior. Offline games have been explored in the form of board [6] or escape room [7] games.

Apart from gamified contexts, **embedded training** has gained momentum in recent phishing intervention research. Embedded training describes interventions that *"train a skill using the associated operational system including software and machines that people normally use"* [4, p. 406]. In other words, embedded training combines testing users' behavior in their normal personal or work environments with instant corrective performance feedback. It has been argued that the experience of "being phished" constitutes a so-called most teachable moment, where lasting change to attitudes and behaviors is possible [13]. Embedded training has been studied by 13 publications in our literature sample. As an example, "PhishGuru" is a program that simulates harmless but realistic phishing emails right into users' email inboxes [44–47]. When falling for a simulated phishing attempt (i.e., clicking



Category	Definition	Phishing interventions	Articles
Education	Educational interventions aim at developing knowledge and understanding of phishing and how to protect oneself against it.		
Education		Text-based, video-based, or in-class education	[8,39,48,63,70,85,95]
Training	Training interventions refer to interactive elements or exercises, which provide users with hands-on practice. They often take place by presenting a realistic phishing attempt within a secure environment.		
Serious game	Serious games refer to gamified contexts in which users can train how to recognize and analyze phishing attacks.	Online game (e.g., "NoPhish"), mobile app, board game, escape room game	[5–7,12,17,21,28,31,32,47,60,71–73,86,88]
Embedded training	Embedded training refers to training schemes that combine testing users' behavior in their normal environment with instant corrective performance feedback.	Phishing simulation in combination with a "teachable moment" (e.g., "PhishGuru")	[4,10,11,13,15,30,44–46,52,75,85,94]
Mindfulness-based training	Mindfulness-based approaches refer to trainings that increase users' awareness of context.	Approaches that teach users to dynamically allocate attention during message evaluation	[40]
Awareness-raising	Awareness-raising interventions refer to warnings that are placed in situ and raise users' awareness of potential phishing attempts during their primary course of action.		
Interactive warning	Interactive warnings refer to awareness-raising interventions that do require user interaction, i.e., interrupt the users' course of action.	Forced-attention warning, security questions, interactive fear appeal	[2,25,29,39,61,62,68,70,75,83,89,93,95,96,98]
Passive warning	Passive warnings refer to awareness-raising interventions that do not require user interaction.	Security toolbar, display of information on the legitimacy of a website	[8,25,92]
Design	Design interventions refer to design choices that aim at supporting or guiding users' behavior with respect to their secure handling of online activities.		
Visual elements	Visual elements refer to interventions that use the visual appearance of, e.g., a login form or website, to support users' security behavior.	UI dressing, dynamic security skins, trust logo, image	[24,34–36,43,49,51,68,81,97]
Color code	Color codes refer to simple visual cues for users to distinguish between secure and risky environments.	Traffic light colors	[43,89,92]
Highlighting	Highlighting refers interventions that draw users' attention towards critical elements.	Domain highlighting, sender highlighting, highlighting differences in out-of-focus tabs	[22,50,56,83]
Customization	Customization refers to interventions that let users customize the visual appearance of, e.g., a login form.	Custom icon, custom image, custom UI dressing	[24,34–36,51,68,81,97]
Redirect users' course of action	This category refers to interventions that redirect users' course of action, for example by offering more secure alternatives.	Browser sidebar for entering credentials, suggesting alternative websites, creating habit of using bookmarks, delayed password disclosure	[35,38,54,66,93]

Figure 2: A taxonomy of user-oriented phishing interventions.

on a phishing link), users were redirected to a training website explaining how phishing attacks work and how they can protect themselves from fraudulent emails and websites. Embedded training is a promising approach with regard to the real-world environment it takes place in: users are not in a training environment (such as an online game), but receive training only if they fall for a simulated phishing attempt during their everyday duties. Thus, knowledge and changes in security attitudes and behaviors can be transferred to real phishing attempts more easily. This is reflected in a growing business of embedded "phishing simulation training" by commercial information security companies [2]. Kumaraguru *et al.* have shown that training with "PhishGuru" helps users retain what they learned in the long term and that multiple training interventions increase performance [44].

Beyond rule-based training, Jensen *et al.* [40] have shown that expanding the rather conventional training toolkit with **mindfulness-based training** leads to a better ability to avoid phishing attacks. Mindfulness training teaches users to dynamically allocate attention during message evaluation (*"(1) Stop! (2) Think ... (3) Check."*) and aims to increase users' awareness of context. This method seems to be particularly effective for participants who were already confident in their detection ability.

3.2.3 Awareness-raising

The third category, awareness-raising, aims at focusing users' attention on potential threats and their countermeasures in situ,

[2]For example, Proofpoint ThreatSim® (proofpoint.com), Sophos Phish Threat (sophos.com), IT-Seal Awareness Academy (it-seal.de), Lucy Security (lucysecurity.com), and many others.

that is, as part of their primary course of action. Awareness-raising interventions might, for example, interrupt the user's workflow to set security-conscious behavior on their agenda. We have identified 17 studies of awareness-raising interventions, of which three explore **passive warnings** (i.e., the warning does not require user interaction), and 15 investigate on **interactive warnings** (i.e., the warning does require user interaction). Several prior studies have shown that passive interventions such as security toolbars in an internet browser are ineffective at preventing phishing attacks [25, 92].

Interactive warnings have been shown to have promising effects on users' phishing vulnerability. For example, the browser sidebar "Web Wallet" [93] acts as a secure way to submit sensitive information by suggesting alternative safe paths to intended websites and forcing users' attention by integrating security questions. Several research works have explored the mechanism of forced attention: Volkamer *et al.* [83] have introduced "TORPEDO", an email client add-in that delays link activation for a short period of time. As for web browser phishing warnings, Egelman *et al.* [25] have shown that interactive warnings, where users have to choose between options such as "Back to safety" or "Continue to Website", are heeded significantly more often compared to passive warnings. Furthermore, Petelka *et al.* [61] have shown that link-focused warnings are more effective than general email banner warnings in protecting users from clicking on malicious URLs, and that forced attention amplifies this effect. When comparing awareness-raising interventions that include educational elements (such as descriptions of the consequences of phishing, or explanations why a certain link or file is classified as potentially dangerous) to those that do not provide any additional information, the former were found to be more effective [75, 95]. Two research works have examined the potential of fear appeals, that is, short, informative messages that communicate threats, and have found that concrete fear appeals (compared with abstract fear appeals) are more effective to increase actual compliance behavior [39, 70]. This indicates that a combination of warning, forcing users' attention, and therein embedded tangible education yields a promising protection against phishing threats.

3.2.4 Design

Lastly, design choices can act as phishing interventions if they facilitate desirable user behavior [39]. We have identified 20 publications that investigate design interventions aimed at supporting users' secure handling of email and online activities.

Visual elements play a role in several research works (10 publications). For instance, the potential of "dynamic security skins" has been explored by Dhamija and Tygar [24], who have presented an authentication scheme where users rely on visual hashes from a trusted source that match the website background for legitimate websites.

Visual elements also come into play when offering users design options to **customize** security indicators, such as custom images or icons. An example is "Passpet", a browser extension by Yee & Sitaker [97] that acts as a password manager and an interactive custom indicator. Iacono *et al.* [36] have proposed so-called "UI-dressing", a mechanism that relies on the idea of individually dressed web applications (e.g., by using customized images) in order to support the user in detecting fake websites.

Color codes refer to simple visual cues (e.g., traffic light colors) for users to distinguish between secure and risky environments. They have, so far, been observed to be of limited success in the form of security indicators that signal whether a website is genuine or fake [43, 92]. Furthermore, Wiese *et al.* [89] have explored color codes in the context of email application UI design, where they were used to indicate the presence of digital signatures.

In contrast, **highlighting** draws users' attention to critical elements. For example, both Volkamer *et al.* [83] and Lin *et al.* [50] have investigated the effectiveness of domain highlighting in order to enable users to find the relevant part of a URL, whereas Nicholson *et al.* [56] have explored highlighting an email's sender name and address.

Other design interventions set out to **redirect users' course of action**, for example, by creating the habit of using browser bookmarks instead of hyperlinks to access sensitive websites such as login pages [35]. Ronda *et al.* [66] have developed "iTrustPage", a tool that warns the user about suspicious websites (e.g., a fake PayPal website). Beyond that, it offers corrective action in the form of suggesting alternative websites that are deemed trustworthy based on Google's search index (e.g., the real PayPal website).

Surprisingly, while the concept of digital nudging has gained widespread attention (among others in usable security research, e.g. [16, 19, 42, 100]) in recent years, only one article in our sample has investigated the effect of a nudge: Next to highlighting the name and address of an email's sender, Nicholson *et al.* [56] have investigated the effect of a social salience nudge ("62% of your colleagues received a version of this email") on users' phishing vulnerability. While several other design interventions contain nudge-like elements (such as color codes or highlighting), none of them have been designed as or labelled a nudge by the respective authors. We will further elaborate on the potential of digital nudging in phishing interventions in Section 4.2.

3.3 Which Phishing Attack Vector Does the Intervention Address?

While the term "phishing" originally describes cyber attacks that aim for users' passwords, it is now used to describe all sorts of attack vectors [23]. Those attack vectors differ in terms of the criminals' intended outcome (e.g., disclosure of confidential information or implanting malware) and the

user's primary action during which the attack takes place (e.g., clicking on a link or downloading a file). In the following, we will analyze the range of attack vectors that the phishing interventions in our sample aim to intervene in detail.

Phishers predominantly choose email messages as their first approach towards the user [85]. About 3.9 billion people worldwide have email accounts and collectively send and receive over 290 billion emails per day [37]. Email thus presents a means of communication that can easily be abused to take advantage of users' credulity by blending into daily personal or professional correspondence. Since attackers employ social engineering techniques (e.g., urgency cues or trustworthy-seeming visual elements) to elicit specific actions such as clicking a link, opening an attachment, or disclosing sensitive information, **deceptive email messages** themselves can be considered as an attack vector. Seventeen publications address users' ability to distinguish legitimate emails from phishing emails by paying attention to the email message itself. For instance, Caputo *et al.* [13] have studied embedded phishing training that aims at educating users on how to recognize phishing emails based on various criteria such as mismatched names, spelling mistakes, or intuition.

Phishing messages furthermore often offer a link, which, for example, might execute a drive-by download of ransomware [85] or redirect the user to a website masquerading as a legitimate login page. Previous research suggests that, after recipients click on a phishing link, they rarely detect subsequent fraudulent attempts such as a counterfeit login page or change their course of action [91]. **Disguised URLs** (such as, e.g., *paypa1.com*, *mybank.com-secure.biz*, or *tinyurl.com/XYZ*), that make the user believe that they are clicking on a reliable link, hence constitute a prominent attack vector. Accordingly, more than half of our literature sample (33 publications) explores user-oriented phishing interventions that aim at preventing users from clicking malicious links. These interventions mostly consider links in the context of an email. For example, Volkamer *et al.'s* [83] email client add-on "TORPEDO" uses tooltips to focus the user's attention on a link's domain. While links with whitelisted or previously visited domains will be activated immediately when clicked, "TORPEDO" will delay the activation of other links for a few seconds to encourage the user to check the URL's domain carefully. Several training games provide users with an in-depth explanation and exercise about how URLs can be obfuscated to mimic reputable sources, and have been shown to help users make better decisions concerning the legitimacy of URLs in the long term (e.g, [12, 72, 76]).

While links are usually accessed via clicking on a link, **QR codes** gain in popularity due to their ease of distribution and fast readability. Since the user has no means to examine the URL behind a QR code before scanning it, they constitute a hidden security threat. One single publication in our sample has addressed this issue by exploring security features of QR code scanners that help users to detect phishing attacks [96].

Besides disguised URLs, **imitated websites** can present another attack vector. For example, cyber criminals employ imitations of well-known websites in order to exploit users' trust in visually familiar or trustworthy environments. Ten publications in our literature sample have addressed this attack vector. For example, Iacono *et al.* [36] have proposed an intervention that relies on the idea that the whole appearance of a web application is dressable according to the user's individual preferences, raising users' attention for unofficial sites that do not align with the expected appearance. Regarding phishing interventions that are being displayed on websites, Kirlappos and Sasse [43] have revealed that arbitrary logos, certifications, or advertisements that do not imply trustworthiness of a website might have a higher reassurance to users than actual security indicators. This gives an example of how user-oriented interventions themselves can be exploited by cyber criminals to trick users into placing trust into a website.

When browsing the internet, interventions such as padlock icons or warning messages inform the user about a website's **SSL/TLS certificates**[3]. Interventions that inform or warn the user about SSL/TLS have been addressed, for example, by Reeder *et al.* [62] or Schechter *et al.* [68]. So-called man-in-the-middle attacks, where criminals use legitimate websites that do not encrypt data transmission by SSL/TLS to capture the user's sensitive data during an online transaction, have been a serious phishing attack vector in the past. Since nowadays, however, more than 80% of phishing sites have SSL/TLS encryption enabled [1], this attack vector will likely cease to play a role in the near future.

We now move from the preliminary stages (such as tricking users into trusting an email, link, or website) to the centerpiece of a phishing attack. One central aspiration of cyber criminals is to lure their victim into disclosing sensitive information, e.g., login credentials. Accordingly, several prior works (12 in our literature sample) have studied interventions that address the process of users' **authentication**. For example, Dhamija & Tygar [24] have introduced an interaction technique for authentication that provides a trusted window in the browser dedicated to username and password entry, which uses a photographic image to create a trusted path between the user and password entry fields. Similarly, Yee & Sitaker's [97] browser extension "Passpet" constitutes a password manager that helps users securely identify trustworthy login forms.

Besides fishing for credential data, phishers' efforts are directed at prompting the user to download or execute **malware**, that is, malicious software that can harm the user's device or their entire network. Malware attacks have rapidly grown over the recent years, e.g., in the form of ransomware attacks [74]. Surprisingly, interventions that aim at preventing users from executing malware are scarce in our literature data. Only three publications have addressed this attack vector: Wen *et al.* [88]

[3] Transport Layer Security (TLS), and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network [57]

have included different kinds of potentially malicious attachments in their conception of a role-play anti-phishing training game, whereas Reeder *et al.* [62] have explored users' interaction with browser warnings that warn against downloading malware. Reinheimer *et al.* [63] have taught how to identify dangerous files in their in-class training.

Malicious **mobile applications** can act as a phishing attack vector, for example, by masquerading as a legitimate online banking app. One publication in our sample has discussed personalized security indicators in mobile applications [51].

In addition to the above-described investigations of specific phishing attack vectors, 10 publications have approached the topic of phishing in a more general manner. Most of these publications have examined training formats, such as online games, that cover the phenomenon of **phishing in a broader sense** without addressing or intervening one attack vector in particular.

Figure 3 illustrates the distribution of our literature data across different phishing attack vectors. Since some publications address interventions to more than one phishing attack vector, the sum of the displayed data points is larger than the literature sample size of 64 articles. For a detailed categorization of all articles, please refer to Table 2 in the appendix.

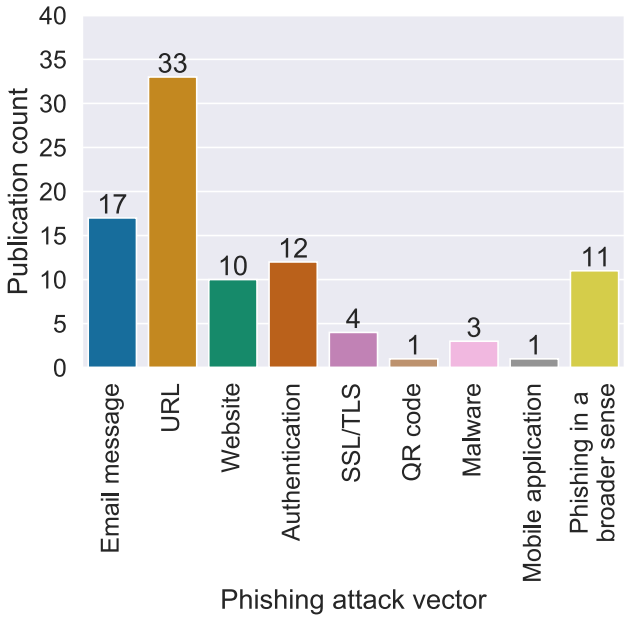


Figure 3: Overview of the attack vectors addressed by phishing interventions studied in the literature data.

3.4 When Does the Intervention Take Place?

Diving deeper into the analysis of user-oriented phishing interventions, we have further considered the point in time at which the intervention takes place. We have found that many interventions, mostly those aiming at training or education, are designed to take place as a precautionary measure, often long before the user interacts with a potential phishing context. We have identified 23 articles that present such interventions and have labeled them as **pre-decision interventions**. For instance, Jansen & van Schaik [39] have shown that confronting users with fear appeal messages is suitable to heighten their cognitions, attitudes, and intentions with regard to secure online behavior. Furthermore, all kinds of non-embedded education or training (e.g., in-class education [48], online games [72], mobile training apps [12]) clearly take place pre-decision.

Most of the approaches in our literature sample focus on interventions that take place during users' course of action, that is, **during the user's decision** between phishing and legitimate content in a real-world context. Those 31 articles mostly describe awareness-raising and design interventions, sometimes combined with educational elements. For instance, Petelka *et al.* [61] have examined the effectiveness of different levels of link-focused warnings when sorting emails, whereas various design interventions such as color codes, customization or highlighting aim to support users' decisions during their course of action.

We have further identified 11 publications describing interventions that take place **post-decision**, that is, after a user's decision on potential phishing contents was already made. This goes especially for embedded training, where training follows right after the user has been "phished" by a simulated attack.

Combinations of pre-, post-, and during decision intervention have been studied only once in our sample: Blythe *et al.* [8] have introduced an approach that consists of initial video-based education, which is then referred back to by security warnings during the users' individual course of action.

While several research works have employed longitudinal studies to examine the long-term effects of user-oriented phishing interventions (see Section 2), little has been investigated on interventions that take place regularly, e.g., by giving regular warnings or recurringly providing users with training. Reinheimer *et al.* [63] have explored the effect of reminding users of initial phishing awareness education and have found that reminders after half a year are recommended and that measures based on videos or interactive examples perform better than text-based reminders. Furthermore, several embedded training interventions have been explored in terms of the effect of recurringly simulated phishing emails (e.g., [13,15,44,52]).

Figure 4 sums up the distribution of the time of intervention across our literature sample.

3.5 Does the Intervention Require User Interaction?

Beyond the categorization as presented in Figure 2, we have analyzed all interventions in terms of whether they require active user interaction, e.g., whether the user's workflow is

Figure 4: The time at which the intervention takes place in relation to the user's decision, across our literature sample.

interrupted by the intervention and whether the user can only proceed when undertaking a certain action or decision. These interventions were classified as **interactive**. In contrast, interventions that only provide information or feedback to the user without actively interrupting their workflow are deemed **passive** interventions. Some of the 64 articles in our literature sample have addressed both interactive and passive interventions.

Across our sample, 48 publications describe phishing interventions that require user interaction. We mainly divide between two kinds of interactive interventions, one being interactive warnings as described in Section 3.2.3, which usually require a few seconds of the user's time and attention before they can proceed with the task at hand (e.g., [25, 61]). The other subset is formed by training and education approaches (see Sections 3.2.1, 3.2.2), which commonly require the user to actively engage in an exercise for at least several minutes up to hours, for example, online training games [12, 31, 72] or in-class training [48]. A total of 16 interventions can be described as passive, including passive warnings (e.g., [92]), some educational interventions (e.g., [39]), and also several interventions belonging to the design category. As an example, we have classified domain highlighting [50] as passive, since it does not require any interaction on the user's side and can also be easily ignored, or even overlooked, by the user.

4 Discussion

In the previous section, we have examined a plethora of user-oriented phishing interventions from various angles and have revealed surprising and relevant insights. Above all, we have found a highly fragmented landscape of educational interventions, training, awareness-raising warnings, and anti-phishing designs, which users need to navigate through when being pushed towards secure online behavior. To summarize and connect the findings across the dimensions of analysis, Figure 5 displays an integrative plot of all phishing interventions in our sample. Getting back to our research questions *RQ1* and *RQ2*, we devote the remainder of this article to discussing our findings and positioning them in current usable security research. After looking at the user effort and intrusiveness of prior phishing interventions in Section 4.1, we discuss the potential of digital nudges regarding phishing prevention in Section 4.2. We then address the role of users' cognitive processes when dealing with potential security threats in Section 4.3. Further, we consider the imbalance of phishing attack vectors addressed by prior intervention research in Section 3.3, and discuss the potential of tailored phishing interventions in Section 4.5. Subsequently, we highlight methodological aspects in Section 4.6, and lastly address limitations of our work in Section 4.7. We then sum up our contributions in Section 5, including an overview of our propositions for future phishing intervention research.

4.1 User Effort and Intervention Intrusiveness

One particularly salient finding is that most user-oriented phishing interventions encumber the user with additional effort with respect to their workload and time, for example, in the form of playing a training game [72], interacting with embedded training [44], answering security questions [93], or waiting for delayed link activation [83]. Those seconds or minutes required to interact with an intervention cumulatively drain time from individual and organizational productivity. Moreover, they often intrusively disrupt the user in their primary goals, hence again substantially decreasing productivity by distraction and potentially leading to stress and frustration. This aligns with Sasse's [67] observation that user time and effort are rarely at the forefront of security studies and that the issue of user effort and intrusiveness has scarcely been considered. Sasse has argued that designers of security tasks should focus on *"causing minimum friction"* and *"must acknowledge and support human capabilities and limitations"* [67, p. 82]. She has called for subjecting security measures to a cost-benefit test and to give up on perfection and focus on essentials. On the other hand, passive, that is, less intrusive interventions have been observed to be of limited success as of yet [36, 43, 68, 92]. It hence remains the most challenging task to design effective user-oriented phishing interventions that prove themselves usable in individuals' everyday online activities, particularly with regard to user effort and intrusiveness. Digital nudging [77, 87] might constitute an unintrusive yet promising approach for this endeavor. In Section 4.2, we evaluate which elements of prior, effective interventions could be classified as nudges retrospectively and present ideas for future approaches. As for training and education interventions, Cranor & Garfinkel [20] have argued that *"the world's future cyber-security depends upon the deployment of security technology that can be broadly used by untrained computer users"*, hence questioning the usability of such approaches. It is still an open question whether interventions need to be understood by the user (e.g., via providing educational information) in order to be effective [25, 100], whereas it has been observed that intervention clearness (e.g., with regard to their message concreteness [70] or their location [61]) increases effectiveness. This spans an interesting research area with potentially crucial insights for the design of future phishing interventions.

Figure 5: Overview of user-oriented phishing intervention literature, spanned by attack vector, time of intervention, and intervention category. Since some articles have addressed several attack vectors or intervention categories, they appear more than once.

4.2 Digital Nudges As Phishing Interventions?

As described in Section 3.2.4, the concept of digital nudging has scarcely been drawn on in phishing intervention research as of yet. The term nudging has been introduced by Thaler & Sunstein [77] in 2009. Digital nudges describe user-interface design elements that target automatic cognitive processes, such as biases or heuristics, to gently push end-users, with little mental effort, to perform the "right" behavior without limiting their choice set [77, 87]. In this section, we aim to discuss the potential of digital nudges in phishing intervention research, especially since prior research in related fields, such as digital privacy-protection or security choices [16, 65, 100], can serve as a solid basis to start from. Surprisingly, phishing intervention literature from 2018 onward has focused on education, training, and awareness-raising measures, while neglecting design interventions (see Table 2 in the appendix). Design phishing interventions might provide significant value to users' security if they succeed in nudging users towards secure behavior, while not being perceived as intrusive with regard to their primary goals.

In an extensive review, Caraban *et al.* [14] have classified six distinct nudge categories in the area of human-computer interactions. In the following, we exemplarily discuss how existing interventions make use of several of those mechanisms already (although not labeling them as nudging) and present novel ideas on how digital nudging could be applied in future phishing intervention research.

Facilitate. Facilitating nudges use mechanisms to lessen users' effort. In our sample, highlighting domains [50, 83] or sender addresses [25] falls in this category since it makes it easier for users to spot the relevant part of an URL or email sender. We propose to take this approach further, for example, by displaying a link's domain next to the link text in an email, with only the domain being clickable.

Confront. Confronting nudges aim to create friction by throttling users' mindless activity or reminding them of the consequences. Several of the interventions in our sample can be described as such, for example, interactive awareness-raising measures as described in Section 3.2.3. As we have argued in the previous section, burdening the user with intrusive distraction and effort cannot be an efficient answer to current and future challenges in cyber security. We hence argue that confronting nudges should be designed to be of minimal possible friction. For example, they could remind the user of consequences by making security risks tangible.

Deceive. Deceptive nudges influence the perception of the available options, e.g., by adding inferior alternatives or placebos. None of the analyzed interventions could be sorted into this category, and we do not deem deceptive nudges suitable for phishing intervention research.

Social Influence. This type of nudge makes use of social influences on people's choices. Examples of social influence within the analyzed articles include the comparison of facts and stories provided by peers vs. experts on anti-phishing education [52] as well as Nicholson *et al.'s* [56] social saliency nudge. Furthermore, social influence has been studied in a social learning environment in terms of gamified elements such as levels or leader boards [73]. Future social influence nudges could provide users with information on, e.g., their vs. their peers' performance in phishing simulations or incident reporting activities.

Fear. Two research works of our sample [39, 70] have introduced fear appeals as phishing interventions with promising results regarding users' protection motivation, attitudes, intentions and compliant behavior. However, both articles have studied fear appeals far from a real-world scenario, using text-based treatments and a survey instrument. We suggest that fear nudges, which, integrated in the user's course of action, aim to invoke fear to encourage a certain choice, are of high interest for future research. Nevertheless, they require ethical considerations [64]. As an example, we imagine a brief but concrete [70] and strong [39] fear appeal next to email

attachments, addressing the risk in terms of financial losses and operational damage coming along with this file type and a potential malware infection. The fear appeal could be framed positively to address ethical concerns by showing how the user could protect against these threats easily.

Reinforce. Reinforcing nudges aim to support certain behaviors, e.g., by ambient feedback or just-in-time prompts. Regarding the first, we found mechanisms ranging from color-coding security indicators on websites [34, 92] to providing customized background images [51, 68] in our sample. One shortcoming of these interventions seems to be that users cannot distinguish between legitimate security indicators (such as a color code) and untrustworthy signs, such as arbitrary logos and certifications [43]. One way to battle this could be to make ambient feedback more comprehensive or standardized, e.g., by color-coding complete email or website windows. Concerning just-in-time prompts, in order to condense prior warning interventions to the pure form of a digital reinforcement nudge, we ideate an authentication intervention that displays the domain of a login website above any login form when placing the cursor in the login field.

Finally, suitable nudges could be easily combined with other interventions types, for example, educational elements [100], as shown by successful examples [39, 70, 95]. As illustrated in Table 2 in the appendix, interventions that combine educational with awareness-raising or design approaches have rarely been studied in phishing research as of yet.

4.3 Shifting Users' Cognitive Frame

From a different perspective, Wash [84] has adduced IT experts' approach towards identifying phishing emails and has observed that experts naturally follow a three-stage process: (1) making sense of the email, relating it to one's personal context, and deriving required action (2) becoming suspicious and investigating, and (3) dealing with the email by deleting or reporting it. He argues that shifting the user's cognitive frame from sensemaking to investigation is crucial for the success of phishing prevention measures. However, half of the interventions in our literature sample have addressed training or education measures (see Figure 5). Those mostly neglect the initial process of noticing slight discrepancies or cues in an email in the sensemaking frame and provide support only in the investigation frame (e.g., how to analyze an URL). While Jensen *et al.'s* [40] mindfulness-based training aims to support users in their awareness of context, and such during their sensemaking process, long-term efficacy is uncertain.

At the same time, users' own security goals should not be neglected: Kirlappos *et al.* [43] have argued that users do not focus on security warnings, but rather look for signs to confirm a website's trustworthiness. For example, users have been shown to trust websites that display advertisements affiliated with known entities or those with familiar website layouts - while both factors do not give evidence of the website's trustworthiness. Therefore, the authors have called for security education to consider the drivers of users' behavior in their respective situation and, conversely, to eliminate users' misconceptions that lead to insecure behavior.

We hence argue that future phishing interventions should strive to meet the user in their own respective sensemaking process, for example, when reading emails, shopping, or doing bank transactions online. Digital nudges might play an important role in this particular case, as well. Supporting the user's cognitive frameshift from the stage of sensemaking to the stage of investigating if certain cues or discrepancies are present will be an important path for future research and will complement the diverse landscape of education and training measures.

4.4 What About Malware?

Regarding the phishing attack vectors addressed across our literature data, we have found that more than half of the interventions focus on the attack vector URL, for example, by training users' skills in analyzing a link or raising their awareness in situ. Interventions supporting the user with deceptive email messages, disguised websites, and fraudulent authentication forms follow by far (see Figure 5).

Malware poses a tremendous risk through current cyber attack patterns [18, 58]. Those attacks are often delivered by archive files or Microsoft Office documents which mimic, e.g., legitimate invoices. Since the user needs to download and open these files on their system, this presents quite a different attack procedure compared with clicking a link. Therefore, it is striking that only three publications have included educational, training, or awareness-raising interventions in their works that address malware alongside other attack vectors. None of the articles in our sample has focused on studying interventions that primarily support users in detecting or handling malware, nor have the challenges of malware interventions compared to previous phishing intervention research been addressed.

We therefore strongly suggest further research to expand previous approaches on phishing interventions in terms of the attack vector by taking into account malicious files and developing interventions that address the actual threat landscape.

4.5 Tailored Interventions

In the context of user interventions in cyber security, several studies have pointed out the potential of personalization regarding user traits [26, 41, 59], or the importance of context (e.g., personal vs. organizational [70]). It has been argued that using tailored instead of one-size-fits-all interventions may enhance their efficacy and user compliance [26].

Interestingly, our literature review does not reveal a strong focus on tailored user interventions to prevent phishing attacks. However, some of the approaches were indeed imple-

mented for specific target groups – mainly for rather heterogeneous groups of employees [73], or children [48]. Since spear phishing attacks are specifically targeted at personal or contextual vulnerabilities, considering users' traits, capabilities and requirements when developing and evaluating user interventions may be a decisive factor for their efficacy, suggesting a scope for future research.

4.6 Methodological Aspects

As described in Section 3.1, current research often lacks realism regarding the experimental setup since it remains challenging to study a phenomenon of deception that usually takes place during users' secondary tasks. Therefore, we argue that future research should not only focus on designing user-oriented phishing interventions, but also on developing experimental setups that account for a realistic analysis of users' security behavior.

Furthermore, we have found that the effect of recurring interventions has been studied scarcely (see Section 3.4). However, many interventions in our sample are designed to train, warn or guide users recurringly. Factors such as habituation [80] or security fatigue hence could have important effects. This proves another major shortcoming in prior phishing intervention research, which should be considered by future works.

4.7 Limitations

In this work, we have carefully selected (usable) security-specific databases to include a large number and variety of publications. Furthermore, the chosen search term was rather broad, and additional sources (such as security conferences) were considered to avoid overlooking relevant findings. Nevertheless, the list of publications analyzed in this research is probably not exhaustive. Furthermore, the features of the different phishing interventions were described in varying detail due to the individual focus and comprehensiveness of the articles. It is thus possible that certain interventions were classified differently by us than the authors themselves would have classified them. Therefore, this systematization of knowledge does not serve as an endpoint but as a starting point for identifying the current state, potential research gaps, and relevant paths for future work. We hope to not only provide a relevant summary and systematization of existing strategies for usable security-related researchers and practitioners but especially to encourage future studies in this increasingly relevant domain, where the human factor plays an essential role.

5 Conclusion

Phishing does not cease to be a threat to both personal and organizational data and operational security. It directly targets the human factor via deceptive emails, attachments, and websites, hence calling for user-oriented interventions that support individuals in recognizing and fending off such attacks. In this work, we have systematically analyzed 64 phishing intervention research articles for methodology, intervention type, attack vector, intervention time and user interaction, and have derived a taxonomy of user-oriented phishing interventions. Connecting the findings across the dimensions of analysis, as well as taking into account current movements in usable security research, we have revealed relevant insights and potential avenues for future work. The latter can be summarized as follows:

Minimize user effort and intervention intrusiveness. How can we design effective phishing interventions that cause minimum friction with the user's course of action and do not cumulatively burden the user with secondary time and workload? Which role does educational information play in intervention effectiveness, compared with intervention clearness and concreteness?

Explore the potential of digital nudging. How can facilitating, confronting, reinforcing, fear, or social influence nudges support users' course of action with regard to secure online behavior?

Help users shift their cognitive frame. How can we support users in the cognitive process of shifting from their primary goal of sensemaking towards noticing discrepancies if "something is off"? How can we transfer experts' expertise with phishing detection into effective end-user interventions?

Protect users from malware attacks. Which kinds of interventions can help to protect users from malware attacks? Which novel challenges do arise for malware-focused interventions, compared with threats employing malicious URLs or websites?

Explore tailored interventions. How can tailored phishing interventions enhance previous approaches?

Develop realistic experimental setups and study long-term effects. Which novel ways can be employed to align experimental setups with the nature of phishing and to account for longitudinal effects?

With this article, we hope to provide a comprehensive starting point as well as inspiration for future user-oriented phishing intervention research.

6 Acknowledgements

This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

[1] Greg Aaron. APWG Phishing Activity Trends 3rd Quarter Report 2020, 2020.

[2] Ahmed Abbasi, F Mariam Zahedi, and Yan Chen. Phishing susceptibility: The good, the bad, and the ugly. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI), pages 169–174. IEEE, 2016.

[3] Luca Allodi, Tzouliano Chotza, Ekaterina Panina, and Nicola Zannone. The need for new antiphishing measures against spear-phishing attacks. IEEE Security & Privacy, 18(2):23–34, 2019.

[4] Abdullah Alnajim and Malcolm Munro. An anti-phishing approach that uses training intervention for phishing websites detection. In 2009 Sixth International Conference on Information Technology: New Generations, pages 405–410. IEEE, 2009.

[5] Nalin Asanka Gamagedara Arachchilage, Steve Love, and Konstantin Beznosov. Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior, 60:185–197, 2016.

[6] Malak Baslyman and Sonia Chiasson. "Smells phishy?": An educational game about online phishing scams. In 2016 APWG Symposium on Electronic Crime Research (eCrime), pages 1–11. IEEE, 2016.

[7] Erwan Beguin, Solal Besnard, Adrien Cros, Barbara Joannes, Ombeline Leclerc-Istria, Alexa Noel, Nicolas Roels, Faical Taleb, Jean Thongphan, Eric Alata, et al. Computer-security-oriented escape room. IEEE Security & Privacy, 17(4):78–83, 2019.

[8] Jim Blythe, Jean Camp, and Vaibhav Garg. Targeted risk communication for computer security. In Proceedings of the 16th international conference on Intelligent user interfaces, pages 295–298, 2011.

[9] Jan vom Brocke, Alexander Simons, Bjoern Niehaves, Bjorn Niehaves, Kai Reimer, Ralf Plattfaut, and Anne Cleven. Reconstructing the giant: On the importance of rigour in documenting the literature search process. In Proceedings of the European Conference on Information Systems (ECIS) 2009, pages 1–12, 2009.

[10] AJ Burns, M Eric Johnson, and Deanna D Caputo. Spear phishing in a barrel: Insights from a targeted phishing campaign. Journal of Organizational Computing and Electronic Commerce, 29(1):24–39, 2019.

[11] Mary B Burns, Alexandra Durcikova, and Jeffrey L Jenkins. What kind of interventions can help users from falling for phishing attempts: A research proposal for examining stage-appropriate interventions. In 2013 46th Hawaii International Conference on System Sciences, pages 4023–4032. IEEE, 2013.

[12] Gamze Canova, Melanie Volkamer, Clemens Bergmann, and Benjamin Reinheimer. NoPhish app evaluation: lab and retention study. In NDSS workshop on usable security, 2015.

[13] Deanna D Caputo, Shari Lawrence Pfleeger, Jesse D Freeman, and M Eric Johnson. Going spear phishing: Exploring embedded training and awareness. IEEE Security & Privacy, 12(1):28–38, 2013.

[14] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pages 1–15, 2019.

[15] Anthony Carella, Murat Kotsoev, and Traian Marius Truta. Impact of security awareness training on phishing click-through rates. In 2017 IEEE International Conference on Big Data (Big Data), pages 4458–4466. IEEE, 2017.

[16] Eun Kyoung Choe, Jaeyeon Jung, Bongshin Lee, and Kristie Fisher. Nudging people away from privacy-invasive mobile apps through visual framing. In Proceedings of the IFIP Conference on Human-Computer Interaction, pages 74–91, Berlin/Heidelberg, Germany, 2013. Springer.

[17] Gokul CJ, Sankalp Pandit, Sukanya Vaddepalli, Harshal Tupsamudre, Vijayanand Banahatti, and Sachin Lodha. Phishy - A serious game to train enterprise users on phishing awareness. In Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts, pages 169–181, 2018.

[18] Cofense. COFENSE Q3 Phishing Review. https://go.cofense.com/wp-content/uploads/pdf/Cofense-Q3_2020_Phishing-Review-report.pdf, 2020. Accessed: 2021-02-15.

[19] Lynne Coventry, Pam Briggs, Debora Jeske, and Aad van Moorsel. SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In International conference of design, user experience, and usability, pages 229–239. Springer, 2014.

[20] Lorrie Faith Cranor and Simson Garfinkel. Security and usability: designing secure systems that people can use. O'Reilly Media, Inc., 2005.

[21] Tom Cuchta, Brian Blackwood, Thomas R Devine, Robert J Niichel, Kristina M Daniels, Caleb H Lutjens, Sydney Maibach, and Ryan J Stephenson. Human Risk Factors in Cybersecurity. In Proceedings of the 20th Annual SIG Conference on Information Technology Education, pages 87–92, 2019.

[22] Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, and Wouter Joosen. Tabshots: Client-side detection of tabnabbing attacks. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, pages 447–456, 2013.

[23] Alan R Dennis and Randall K Minas. Security on autopilot: Why current security theories hijack our thinking and lead us astray. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 49(SI):15–38, 2018.

[24] Rachna Dhamija and J Doug Tygar. The battle against phishing: Dynamic security skins. In Proceedings of the 2005 symposium on Usable privacy and security, pages 77–88, 2005.

[25] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 1065–1074, 2008.

[26] Serge Egelman and Eyal Peer. The myth of the average user: Improving privacy and security systems through individualization. Proceedings of the 2015 New Security Paradigms Workshop, pages 16–28, 2015.

[27] EUROPOL. World's most dangerous malware EMOTET disrupted through global action. https://www.europol.europa.eu/newsroom/news/worlds-most-dangerous-malware-emotet-disrupted-through-global-action. Accessed: 2021-02-08.

[28] Rubia Fatima, Affan Yasin, Lin Liu, and Jianmin Wang. How persuasive is a phishing email? A phishing game for phishing awareness. Journal of Computer Security, 27(6):581–612, 2019.

[29] Sophie Gastellier-Prevost, Gustavo Gonzalez Granadillo, and Maryline Laurent. A dual approach to detect pharming attacks at the client-side. In 2011 4th IFIP International Conference on New Technologies, Mobility and Security, pages 1–5. IEEE, 2011.

[30] Kristen K Greene, Michelle P Steves, Mary F Theofanos, and Jennifer Kostick. User context: an explanatory variable in phishing susceptibility. In in Proc. 2018 Workshop Usable Security, 2018.

[31] M Hale and R Gamble. Toward increasing awareness of suspicious content through game play. In 2014 IEEE World Congress on Services, pages 113–120. IEEE, 2014.

[32] Matthew L Hale, Rose F Gamble, and Philip Gamble. CyberPhishing: A game-based platform for phishing awareness testing. In 2015 48th Hawaii International Conference on System Sciences, pages 5260–5269. IEEE, 2015.

[33] Farkhondeh Hassandoust, Angsana A Techatassanasoontorn, and Harminder Singh. Information Security Behaviour: A Critical Review and Research Directions. In Proceedings of the European Conference on Information Systems (ECIS) 2020, 2020.

[34] Amir Herzberg and Ahmad Jbara. Security and identification indicators for browsers against spoofing and phishing attacks. ACM Transactions on Internet Technology (TOIT), 8(4):1–36, 2008.

[35] Amir Herzberg and Ronen Margulies. Forcing Johnny to login safely. Journal of Computer Security, 21(3):393–424, 2013.

[36] Luigi Lo Iacono, Hoai Viet Nguyen, Tobias Hirsch, Maurice Baiers, and Sebastian Möller. UI-Dressing to detect Phishing. In 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS), pages 747–754. IEEE, 2014.

[37] The Radicati Group Inc. Email statistics report, 2019-2023 Executive Summary. https://www.radicati.com/?download=email-statistics-report-2019-2023, 2019. Accessed: 2021-02-08.

[38] Markus Jakobsson and Steven Myers. Delayed password disclosure. ACM SIGACT News, 38(3):56–75, 2007.

[39] Jurjen Jansen and Paul van Schaik. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. International Journal of Human-Computer Studies, 123:40–55, 2019.

[40] Matthew L Jensen, Michael Dinger, Ryan T Wright, and Jason Bennett Thatcher. Training to mitigate phishing attacks using mindfulness techniques. Journal of Management Information Systems, 34(2):597–626, 2017.

[41] Debora Jeske, Lynne Coventry, and Pam Briggs. Nudging whom how : IT proficiency , impulse control and secure behaviour. In Proceedings of the CHI Workshop on Personalizing Behavior Change Technologies, pages 1–4, 2014.

[42] Shipi Kankane, Carlina DiRusso, and Christen Buckley. Can we nudge users toward better password management? an initial study. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, pages 1–6, 2018.

[43] Iacovos Kirlappos and M Angela Sasse. Security education against phishing: A modest proposal for a major rethink. IEEE Security & Privacy, 10(2):24–32, 2011.

[44] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In Proceedings of the 5th Symposium on Usable Privacy and Security, pages 1–12, 2009.

[45] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Protecting people from phishing: the design and evaluation of an embedded training email system. In Proceedings of the SIGCHI conference on Human factors in computing systems, pages 905–914, 2007.

[46] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Lessons from a real world evaluation of anti-phishing training. In 2008 eCrime Researchers Summit, pages 1–12. IEEE, 2008.

[47] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT), 10(2):1–31, 2010.

[48] Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. How Effective is Anti-Phishing Training for Children? In Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security, SOUPS '17, page 229–239, USA, 2017. USENIX Association.

[49] Linfeng Li, Marko Helenius, and Eleni Berki. A usability test of whitelist and blacklist-based anti-phishing application. In Proceeding of the 16th International Academic MindTrek Conference, pages 195–202, 2012.

[50] Eric Lin, Saul Greenberg, Eileah Trotter, David Ma, and John Aycock. Does domain highlighting help people identify phishing sites? In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 2075–2084, 2011.

[51] Claudio Marforio, Ramya Jayaram Masti, Claudio Soriente, Kari Kostiainen, and Srdjan Čapkun. Evaluation of personalized security indicators as an anti-phishing mechanism for smartphone applications. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pages 540–551, 2016.

[52] John Marsden, Zachary Albrecht, Paula Berggren, Jessica Halbert, Kyle Lemons, Anthony Moncivais, and Matthew Thompson. Facts and Stories in Phishing Training: A Replication and Extension. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, pages 1–6, 2020.

[53] Matthew DF McInnes, David Moher, Brett D Thombs, Trevor A McGrath, Patrick M Bossuyt, Tammy Clifford, Jérémie F Cohen, Jonathan J Deeks, Constantine Gatsonis, Lotty Hooft, et al. Preferred reporting items for a systematic review and meta-analysis of diagnostic test accuracy studies: the PRISMA-DTA statement. Jama, 319(4):388–396, 2018.

[54] Daisuke Miyamoto, Takuji Iimura, Gregory Blanc, Hajime Tazaki, and Youki Kadobayashi. Eyebit: Eye-tracking approach for enforcing phishing prevention habits. In 2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), pages 56–65. IEEE, 2014.

[55] David Moher, Alessandro Liberati, Jennifer Tetzlaff, Douglas G Altman, Prisma Group, et al. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS med, 6(7):e1000097, 2009.

[56] James Nicholson, Lynne Coventry, and Pam Briggs. Can We Fight Social Engineering Attacks by Social Means? Assessing Social Salience as a Means to Improve Phish Detection. In Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security, SOUPS '17, page 285–298, USA, 2017. USENIX Association.

[57] Rolf Oppliger. SSL and TLS: Theory and Practice. Artech House, 2016.

[58] Constantinos Patsakis and Anargyros Chrysanthou. Analysing the fall 2020 Emotet campaign. arXiv preprint arXiv:2011.06479, 2020.

[59] Eyal Peer, Serge Egelman, Marian Harbach, Nathan Malkin, Arunesh Mathur, and Alisa Frik. Nudge

Me Right: Personalizing Online Nudges to People's Decision-Making Styles. SSRN Electronic Journal, 2019.

[60] Evan K Perrault. Using an interactive online quiz to recalibrate college students' attitudes and behavioral intentions about phishing. Journal of Educational Computing Research, 55(8):1154–1167, 2018.

[61] Justin Petelka, Yixin Zou, and Florian Schaub. Put your warning where your link is: Improving and evaluating email phishing warnings. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pages 1–15, 2019.

[62] Robert W Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. An experience sampling study of user reactions to browser warnings in the field. In Proceedings of the 2018 CHI conference on human factors in computing systems, pages 1–13, 2018.

[63] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana von Landesberger, and Melanie Volkamer. An investigation of phishing awareness and education over time: When and how to best remind users. In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020), pages 259–284, 2020.

[64] Karen Renaud and Marc Dupuis. Cyber security fear appeals: Unexpectedly complicated. In Proceedings of the New Security Paradigms Workshop, pages 42–56, 2019.

[65] Karen Renaud and Verena Zimmermann. Nudging folks towards stronger password choices: providing certainty is the key. Behavioural Public Policy, 3(2):228–258, 2019.

[66] Troy Ronda, Stefan Saroiu, and Alec Wolman. Itrustpage: a user-assisted anti-phishing tool. ACM SIGOPS Operating Systems Review, 42(4):261–272, 2008.

[67] Angela Sasse. Scaring and bullying people into security won't work. IEEE Security & Privacy, 13(3):80–83, 2015.

[68] Stuart E Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The emperor's new security indicators. In 2007 IEEE Symposium on Security and Privacy (SP'07), pages 51–65. IEEE, 2007.

[69] Guido Schryen, Gerit Wagner, Alexander Benlian, and Guy Paré. A knowledge development perspective on literature reviews: Validation of a new typology in the is field. Communications of the AIS, 46, 2020.

[70] Sebastian W Schuetz, Paul Benjamin Lowry, Daniel A Pienta, and Jason Bennett Thatcher. The effectiveness of abstract versus concrete fear appeals in information security. Journal of Management Information Systems, 37(3):723–757, 2020.

[71] Michael James Scott, Gheorghita Ghinea, and Nalin Asanka Gamagedara Arachchilage. Assessing the role of conceptual knowledge in an anti-phishing educational game. In 2014 IEEE 14th International Conference on Advanced Learning Technologies, pages 218–218. IEEE, 2014.

[72] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In Proceedings of the 3rd symposium on Usable privacy and security, pages 88–99, 2007.

[73] Mario Silic and Paul Benjamin Lowry. Using design-science based gamification to improve organizational security training and compliance. Journal of Management Information Systems, 37(1):129–161, 2020.

[74] Michael Sorensen. The new face of phishing. https://apwg.org/the-new-face-of-phishing/, 2018. Accessed: 2021-01-13.

[75] Nathalie Stembert, Arne Padmos, Mortaza S Bargh, Sunil Choenni, and Frans Jansen. A study of preventing email (spear) phishing by enabling human intelligence. In 2015 European Intelligence and Security Informatics Conference, pages 113–120. IEEE, 2015.

[76] Simon Stockhardt, Benjamin Reinheimer, Melanie Volkamer, Peter Mayer, Alexandra Kunz, Philipp Rack, and Daniel Lehmann. Teaching phishing-security: which way is best? In IFIP International Conference on ICT Systems Security and Privacy Protection, pages 135–149. Springer, 2016.

[77] Richard H Thaler and Cass R Sunstein. Nudge: Improving decisions about health, wealth, and happiness. Penguin, 2009.

[78] Ke Tian, Steve T. K. Jan, Hang Hu, Danfeng Yao, and Gang Wang. Needle in a Haystack: Tracking Down Elite Phishing Domains in the Wild. In Proceedings of the Internet Measurement Conference 2018, IMC '18, page 429–442, New York, NY, USA, 2018. Association for Computing Machinery.

[79] Paul Van Schaik, Debora Jeske, Joseph Onibokun, Lynne Coventry, Jurjen Jansen, and Petko Kusev. Risk

perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior, 75:547–559, 2017.

[80] Anthony Vance, Jeffrey L Jenkins, Bonnie Brinton Anderson, Daniel K Bjornn, and C Brock Kirwan. Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. MIS Quarterly, 42(2):355–380, 2018.

[81] Gaurav Varshney, Anjali Sardana, and Ramesh Chandra Joshi. Secret information display based authentication technique towards preventing phishing attacks. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pages 602–608, 2012.

[82] Rakesh Verma and Keith Dyer. On the Character of Phishing URLs: Accurate and Robust Statistical Learning Classifiers. In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, CODASPY '15, page 111–122, New York, NY, USA, 2015. Association for Computing Machinery.

[83] Melanie Volkamer, Karen Renaud, Benjamin Reinheimer, and Alexandra Kunz. User experiences of TORPEDO: tooltip-powered phishing email detection. Computers & Security, 71:100–113, 2017.

[84] Rick Wash. How Experts Detect Phishing Scam Emails. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2):1–28, 2020.

[85] Rick Wash and Molly M Cooper. Who provides phishing training? facts, stories, and people like me. In Proceedings of the 2018 chi conference on human factors in computing systems, pages 1–12, 2018.

[86] Patrickson Weanquoi, Jaris Johnson, and Jinghua Zhang. Using a Game to Teach About Phishing. In Proceedings of the 18th Annual Conference on Information Technology Education, pages 75–75, 2017.

[87] Markus Weinmann, Christoph Schneider, and Jan Vom Brocke. Digital nudging. Business & Information Systems Engineering, 58(6):433–436, 2016.

[88] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pages 1–12, 2019.

[89] Oliver Wiese, Joscha Lausch, Jakob Bode, and Volker Roth. Beware the downgrading of secure electronic mail. In Proceedings of the 8th Workshop on Socio-Technical Aspects in Security and Trust, pages 1–9, 2018.

[90] Ryan Wright, Kent Marett, and Jason Thatcher. Extending Ecommerce Deception Theory to Phishing. In Proceedings of the 35th International Conference on Information Systems, 2014.

[91] Ryan T Wright and Kent Marett. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. Journal of Management Information Systems, 27(1):273–303, 2010.

[92] Min Wu, Robert C Miller, and Simson L Garfinkel. Do security toolbars actually prevent phishing attacks? In Proceedings of the SIGCHI conference on Human Factors in computing systems, pages 601–610, 2006.

[93] Min Wu, Robert C Miller, and Greg Little. Web wallet: preventing phishing attacks by revealing user intentions. In Proceedings of the second symposium on Usable privacy and security, pages 102–113, 2006.

[94] Aiping Xiong, Robert W Proctor, Weining Yang, and Ninghui Li. Embedding training within warnings improves skills of identifying phishing webpages. Human factors, 61(4):577–595, 2019.

[95] Weining Yang, Aiping Xiong, Jing Chen, Robert W Proctor, and Ninghui Li. Use of phishing training to improve security warning compliance: evidence from a field experiment. In Proceedings of the hot topics in science of security: symposium and bootcamp, pages 52–61, 2017.

[96] Huiping Yao and Dongwan Shin. Towards preventing qr code based attacks on android phone using security warnings. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, pages 341–346, 2013.

[97] Ka-Ping Yee and Kragen Sitaker. Passpet: convenient password management and phishing protection. In Proceedings of the second symposium on Usable privacy and security, pages 32–43, 2006.

[98] Chuan Yue. Preventing the revealing of online passwords to inappropriate websites with logininspector. In Presented as part of the 26th Large Installation System Administration Conference (LISA), pages 67–81, 2012.

[99] Leah Zhang-Kennedy and Sonia Chiasson. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. ACM Computing Surveys (CSUR), 54(1):1–39, 2021.

[100] Verena Zimmermann and Karen Renaud. The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions. ACM Transactions on Computer-Human Interaction, 28:7:1 – 7:45, 2021.

Appendix

Database	After search	After exclusion
ACM	270	35
IEEE	869	15
Web of Science	970	25
NDSS/(Euro)USEC	5	2
USENIX Security/SOUPS	8	3
Other	2	2

Table 1: Number of articles included in the literature review before and after applying the exclusion criteria during the screening of title and abstract.

Author	Sample Size	Lab Study	Online Study	Field Study	Survey	Conceptual	Education	Training	Awareness-raising	Design	Email	URL	Website	Authentication	SSL	Other	Pre-Decision	During Decision	Post-Decision	Interactive	Passive	Educational	Non-Educational
		Method					Intervention Category				Attack Vector						Time of Interv.			Activity		Educ.	
Abbasi et al. [2]	509		•						•			•	•					•		•			•
Alnajim & Munro [4]	36	•						•				•	•						•	•		•	
Arachilage et al. [5]	20	•						•									•			•		•	
Baslyman & Chiasson [6]	21	•						•									•			•		•	
Beguin et al. [7]	14	•						•									•			•		•	
Blythe et al. [8]	/					•	•		•								•	•		•		•	
Burns et al. [10]	400			•				•			•	•							•	•		•	
Burns et al. [11]	/					•		•									•			•		•	
Canova et al. [12]	19	•	•					•				•					•			•		•	
Caputo et al. [13]	1,359			•				•			•	•							•	•		•	
Carella et al. [15]	150			•				•									•			•		•	
Cuchta et al. [21]	4,777			•				•			•	•							•	•		•	
De Ryck et al. [22]	/					•				•			•					•			•		•
Dhamija & Tygar [24]	/					•				•				•				•			•		•
Egelman et al. [25]	60	•							•				•					•		•	•		•
Fatima et al. [28]	63	•						•									•			•		•	
Gastellier-Prevost et al. [29]	/					•			•				•					•		•			•
Gokul et al. [17]	8,071		•					•				•					•			•		•	
Greene et al. [30]	ca. 70			•	•			•			•								•		•		•
Hale et al. [32]	/					•		•									•			•		•	
Hale & Gamble [31]	/					•		•									•			•		•	
Herzberg & Jbara [34]	23	•								•		•			•			•			•		•
Herzberg & Margulies [35]	400			•						•				•				•		•			•
Iacono et al. [36]	18		•							•			•					•			•		•
Jakobsson & Myers [38]	/					•				•				•				•			•		•
Jansen & van Schaik [39]	786				•		•		•					•			•				•	•	
Jensen et al. [40]	355			•				•			•	•					•			•		•	
Kirlappos & Sasse [43]	36		•							•			•					•		•		•	
Kumaraguru et al. [47]	4,517			•				•			•	•							•	•		•	
Kumaraguru et al. [44]	515		•					•			•	•							•	•		•	
Kumaraguru et al. [46]	311			•				•			•	•							•	•		•	
Kumaraguru et al. [45]	30	•						•			•	•							•		•	•	
Lastdrager et al. [48]	353	•					•				•	•	•				•			•		•	
Li et al. [49]	20	•								•		•	•					•		?	?	?	?
Lin et al. [50]	22	•								•		•						•			•		•
Marforio et al. [51]	221	•								•								•			•		•
Marsden et al. [52]	11,968		•					•				•							•	•		•	
Miyamoto et al. [54]	23	•								•		•		•				•		•			•
Nicholson et al. [56]	279		•							•	•							•			•		•
Perrault [60]	462				•			•			•	•					•			•		•	
Petelka et al. [61]	701		•						•			•						•		•			•
Reeder et al. [62]	773			•					•					•	•	•		•		•		?	?
Reinheimer et al. [63]	409			•			•					•				•	•			•		•	
Ronda et al. [66]	2,050			•						•				•				•			•	•	
Schechter et al. [68]	67	•							•	•		•	•	•				•		•			•
Schuetz et al. [70]	264		•				•		•								•			•		•	
Scott et al. [71]	/					•		•				•					•			•		•	
Sheng et al. [72]	42	•						•				•					•			•		•	
Silic & Lowry [73]	384			•				•			•	•					•			•		•	
Stembert et al. [75]	24	•						•	•		•	•						•		•	•	•	
Stockhardt et al. [76]	81	•						•				•					•			•		•	
Varshney et al. [81]	/					•				•				•				•			•		•
Volkamer et al. [83]	16			•					•	•		•						•		•		•	
Wash & Cooper [85]	1,945			•			•	•			•	•							•	•		•	
Weanquoi et al. [86]	/					•		•									•			•		•	
Wen et al. [88]	39	•						•			•	•				•	•			•		•	
Wiese et al. [89]	18		•						•	•	•							•		•		•	
Wu et al. [93]	21	•							•	•				•				•		•		•	
Wu et al. [92]	30	•							•	•		•			•			•			•		•
Xiong et al. [94]	639		•					•				•						•		•		•	
Yang et al. [95]	63			•			•		•			•						•		•		•	
Yao & Shin [96]	20	•							•							•		•		•		•	
Yee et al. [97]	/					•				•				•				•		•		•	
Yue et al. [98]	/					•			•					•				•		•			•
Sum (N=64)		20	12	16	3	13	7	31	17	20	17	33	10	12	4	4	23	31	11	48	16	43	19

Table 2: Results of the literature review, sorted alphabetically by first author.