EYE-TRACKING IN ASSOCIATION WITH PHISHING CYBER ATTACKS: A COMPREHENSIVE LITERATURE REVIEW

Noon Hussein

Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada

ABSTRACT

As of 2021, it has been reported that around 90% of data breaches occur on ac- count of phishing, while about 83% of organizations experienced phishing attacks [1]. Phishing can be defined as the cybercrime in which a target is contacted through e-mail, telephone or text message by someone impersonating a legitimate institution [2]. Through psychological manipulation, the threat actor attempts to deceive users into providing sensitive information, thereby causing financial and intellectual property losses, reputational damages, and operational activity disruption. In this light, this paper presents a comprehensive review of eye-tracking in association with phishing cyberattacks. To determine their impact on phishing detection accuracy, this work reviews 20 empirical studies which measure eye-tracking metrics with respect to different Areas of Interest (AOIs). The described experiments aim to produce simple cognitive user reactions, examine concentration, perception and trust in the system; all in which determine the level of susceptibility to deception and manipulation. Results suggest that longer gaze durations on AOIs, characterized by higher attention control, are strongly correlated with detection accuracy. Eye-tracking behavior also shows that technical background, domain knowledge, experience, training, and risk perception con- tribute to mitigating these attacks. Meanwhile, Time to First Fixation (TTFF), entry time and entry sequence data yielded inconclusive results regarding the impact on susceptibility to phishing attacks. The results aid in designing user-friendly URLs, visual browsing aids, and embedded and automated authentication systems. Most importantly, these findings can be used to establish user awareness through the development of training programs.

be used to establish user awareness through the development of training programs.

KEYWORDS

Cybersecurity, Eye-Tracking, Phishing & Human Factors.

1. INTRODUCTION

According to recent security research, most companies have unprotected data and poor cybersecurity practices in place [3], which highly exposes them to security breaches. As the most common type of cyberattack, phishing describes the attempt to acquire sensitive information by disguising as a credible entity through e-mail, SMS, or phone. By creating a feeling of urgent necessity, inducing curiosity or fear in recipients, victims may reveal sensitive information, click on malicious links, or open attachments that may compromise their machines. As reported by the FBI's Internet Crime 3 (IC3), phishing was the most common cybercrime in 2020 [4]. In particular, one in every 99 e-mails is classified as a phishing e-mail, which makes it the most

David C. Wyld et al. (Eds): CCNET, AIMLA, CICS, IOTBS, NLTM, COIT - 2023
pp. 71-85, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.130406

common social engineering attack, comprising about 90% of security data breaches according to Cisco's 2021 Cybersecurity Threat Trends report [5].

Eye-tracking measures provide valuable non-invasive indices of human brain cognition. Based on gaze analysis, attentional focus and cognitive strategies are revealed. As the most commonly utilized ocular measure, eye gaze carries several advantages over EEG and fMRI for a number of paradigms and research questions.

Firstly, eye-tracking devices enable subjects to be comfortably seated or move freely with head-mounted devices during data collection. This results in a more natural and less space-restricted experimental environment compared to an MRI scanner. Secondly, since most eye-trackers are portable [6], it is easier to form larger and more diverse sample sizes, rather than being limited to subjects who are willing and able to commute to research facilities. Thirdly, the quick process of calibration on modern eye-trackers minimize pre-experiment set-up tasks and testing time.

Multiple gaze metrics used to assess cognition are derived from gaze position data. Gaze position measurements assess the thought process in a moment-by-moment manner for a variety of contexts. Fixations are used in the calculation of time spent looking at a particular location, which reflects engagement of attention as well as time required to process that stimulus. From these metrics, researchers can gain insights into memory [7], processes of mental computations and reading [8,9], in addition to problem-solving and learning strategies [10,11].

Modern web browsers embed tools to aid users in making informed security decisions. For instance, visual indicators can be found within URL bars, whereas SSL padlocks allow for judging the legitimacy of websites. Unfortunately, these indicators have only shown partial success at phishing prevention. Aside to that, poor usability may become advantageous to phishers when masquerading as legitimate sources. As earlier security indicators have proven ineffectiveness, they pose a higher risk of falling victim to phishing. This is compounded by the fact that most users consider security a secondary task [12], which affects the likelihood of noticing security indicators. Furthermore, some security indicators are only visible when the content is secure, which makes the absence of security indicators even less likely to be acknowledged.

Given the serious potential consequences of phishing cyberattacks, it has become of conspicuous interest to deepen one's understanding of the impact of exploited human cognition factors on these attacks, in order to minimize or mitigate their repercussions. In this light, this paper reviews the impact of eye-tracking, mainly including gaze position and associated metrics, on the susceptibility to phishing cyberattacks.

To the best of my knowledge, this is the first paper to review phishing susceptibility through the lens of eye-tracking. After thoroughly searching key academic databases, a full range of journal articles between 2012 and 2022 addressing the application of eye-tracking technology in phishing detection was systematically assessed. Based on rigorous selection criteria, 20 eligible articles were selected for final review, as this study develops a taxonomy built upon a comprehensive range of scholarly journals.

The remainder of this paper is organized as follows: methods for independent and dependent variable measurement are described in Section 2. Section 3 comprises the key findings of the literature, whereas discussions and implications are detailed in Sections 4 and 5, respectively. Limitations of the reviewed studies are presented in Section 6. Lastly, conclusions are reported in Section 7.

2. MEASUREMENT METHODS

Eye-tracking measures the point of gaze and eye motion relative to the head. An eye-tracker is therefore capable of producing a gaze path video and large quantities of physiological data related to attention as well as emotion. These devices come in a mobile or stationary format depending on the focus of the experiment. For example, glasses (mobile) can give insight on attention, response placement of products or other stimuli. To investigate the impact of factors extracted from eye-tracking on susceptibility to phishing, 20 empirical studies [13-32] were reviewed.

Phishing stimuli presented to users at random comprised the independent variable in the experiments, which were typically within-subject studies. Timestamp, gaze position relative to phishing stimuli (X and Y), position in eye-tracker field of view (X and Y), pupil size, and validity code of each eye are parameters measured by eye-trackers. From these, different measurement metrics were derived in the studies, whereas Areas of Interest (AOIs) were used to link them to parts of the used stimulus. For the reviewed work, Table 1 summarizes common AOIs used to evaluate susceptibility to phishing e-mails.

Table 1. AOIs for phishing e-mail detection based on eye-tracking.

AOI	Description
E-mail address	• Attacker disguises themselves as a trusted source. • Engagement is more likely with this form of deception, especially if the source is “familiar” to the user. • Domain or entire e-mail could be spoofed.
Subject line	Exploits urgency, personalization and pressure
Addressee	• Gathered background information about the victim can be used to personalize the attack, therefore increasing susceptibility. • May also be addressed through generalized information from a trusted organization in which they are inclined to comply
Instruction line	• Generally highly personalized to appeal to targets. • Persuasiveness is enhanced by source address spoofing and shortened URLs to hide the destination of the link. • Decisions are made based on previous experiences, biases, or beliefs.

Adding to the above AOIs, the National Cyber Security Centre described financial information, misspelling, threat, and urgency as elements identified in public guidance on possible phishing e-mail indicators [33]. In addition, more specific AOIs were established in the literature for phishing URLs, as described in Table 2.

Table 2. AOI for phishing URL detection based on eye-tracking.

URL AOI	Description
Scheme	• Captures the scheme component and corresponding delimiters. • HTTPS is mainly used as the scheme.
Authority	• Fully qualified domain name (e.g., www.google.com is the authority component of https://www.google.com). • Or has form user@host (e.g., www.google.com@evil.com). • Can be split into user and host AOIs corresponding to user and host components.
Rest	Captures the rest component.
Response	Captures participant response for phishing e-mail classification.
Visual	Captures visual targets other than the aforementioned AOIs, such as: • Trusted Digital Certificate indicator in the web page; lock icon with a green background. • SSL/TLS encryption indicator. • Content quality and information on page.

To measure AOIs, static and dynamic measurement metrics were used. Static metrics were studied in [13], [14] and [20-22], which include personal attributes, such as name, gender, age, income, experience, knowledge, biometric identities, and ethnicity. Although gender and age were somewhat considered, static metrics were not strictly taken into account in the literature, and may be considered as secondary metrics when measuring such physiological factor. Instead, Table 3 describes main dynamic metrics found in the literature.

Table 3. Measurement metrics for eye-tracking-based phishing detection.

Metric	Description
Time to First Fixation (TTFF)	Time taken to look at the first AOI.
Gaze position	Point of gaze; where one is looking.
Fixation count	Denotes interest in a particular content.
Number of regressions	• Number of times a participant returned their gaze to a particular spot, defined by an AOI. • Indicates that the area drew attention and needed further scrutiny.
Glance duration	• Denotes depth of processing. • Characterized by a threshold of 100 ms in [18] and 500 ms in [13].
Entry time and entry sequence	• Time and fixation number that an area was attended to, respectively. • Denotes ease of attentional capture.
Total dwell time	Time taken to fully analyze one item.
Total time	Total time taken to finish the experiment.
Questionnaire	• Related to personal static features, security knowledge and behavior, eye-tracking experience, and others. • One pre-task questionnaire in [18] assessed mood along six emotional states using a 10-point scale to neutralize it before the tasks. • A sample questionnaire can be found in the appendices of [21].

After acquiring gaze data, datasets were usually extended by considering additional metrics (described in Table 3) that build upon the fundamental data. Other metrics used in few studies include times of clicks [18], actions taken (e.g, deleted/archived mail or helpdesk notification) [29], memory [22,32], and pupil size [18], [29], [32] to evaluate user susceptibility from static and dynamic metrics. It is to be noted that although static metrics were not necessarily primary metrics in these experiments, they contributed to unexpected, complex and inconsistent results in relation to susceptibility, as highlighted in the following sections.

Eye-tracking devices used in the experiments are classified into mobile and stationary devices [34]. As compared to mobile eye-trackers, stationary eye trackers can only be used in a laboratory. To further visualize the experimental setting, a brief comparison of used eye-trackers in terms of frequency and accuracy is presented in Table 4.

Table 4. Frequency and accuracy characteristics of eye-tracking devices in experiments.

Study	**Device**	**Type**	**Frequency (Hz)**	**Accuracy (^{o})**
[13]	iMotions SMI RED 500	Stationary	500	0.4
[14], [19]	Tobii Pro Glasses 2*	Mobile (glasses)	100 [14], unspecified [19]	0.62
[15]	Tobii Pro TX300*	Stationary	Unspecified	0.5
[16], [23]	Tobii Pro X2-30*	Mobile (screen	Unspecified [16], 30 [23]	0.4
[17]	Tobii Pro T60XL*	Stationary	60	0.5
[18]	Ergoneers Dikablis Glasses	Mobile (glasses)	60	0.3
[20]	Tobii 1750*	Stationary	100	0.5
[21]	iMotions The Eye Tribe Tracker*	Mobile (screen)	60	0.5
[27]	JINS MEME	Mobile (glasses)	Roughly over 100	Unspecified
[28]	EyeLink 1000 Plus	Stationary	60	0.5
[29]	EyeTech DS TM3	Stationary	60	0.5
[26], [30], [32]	Tobii T120*	Stationary	Unspecified [26], [30], 60 [32]	0.5

*Discontinued

From the table, it can be inferred that: (1) stationary and mobile eye-trackers are almost equally as popular for such experiment, with Tobii eye-trackers being the most used, and (2) eye movements were mostly recorded at 60 Hz, whereas (3) the majority of eye-trackers used had an accuracy of 0.5°.

3. KEY FINDINGS

The key findings of reviewed studies are summarized in Table 5, where some common themes were observed. Firstly, technical attributes, which are described as form and content-related aspects of crafted phishing attacks majorly impacted user behavior. Users paid most attention to salient design elements, spelling, URLs, sender’s address, personalized content, interface and security indicators. As a result, their decisions were highly impacted by their perceived legitimacy of these attributes.

Secondly, personal attributes contributed to the correct identification of phishing attacks. As suggested by the literature, users of technical background, domain knowledge, experience, attention control and risk perception showed higher attentiveness levels, resulting in higher detection accuracy. In addition, contradictory to assumptions, agreeableness was found to have little to no impact on susceptibility to these attacks, as no distinguishable trends from eye-tracking results could conclude otherwise. Although personal attributes can be rather difficult to change, adequate training can decrease susceptibility to phishing attacks. Specifically, training users to be more attentive and critical of phishing AOIs, even if short, enhances the ability to detect phishing cues.

Finally, although the initial fixation on an AOI differed depending on personal and technical attributes, findings suggest that glance duration was dominated by domain names in phishing e-mails and URLs in phishing websites. However, when facing warnings or threats, glance duration was found to be the highest among these. Experimental results contradict some assumptions that warnings and threats may divert attention away from important security indicators or pressure users into complying with attackers' demands. As supported by evidence, users have classified this type of information as less trustworthy, and were more attentive to cues in security warnings, which activated pattern matching mechanisms and induced a positive behavior towards phishing attacks. All in all, a user of a high detection accuracy is characterized by high attention control; spending more time looking at an AOI. Personal attributes have also resulted in secure behavior which contributed to phishing mitigation. Contrarily, TTFF, entry time and entry sequence data yielded inconclusive results regarding impact on susceptibility to phishing attacks.

Table 5. Key findings of reviewed studies.

Study	**Methodology and Sample Size**	**Key Findings**
[13]	Experiment, 22 participants	• Users spent less time looking at phishing indicators than expected. • Financial phishing e-mail indicators yielded the least frequent number of fixations and the least overall dwell time compared to those with misspelling, urgency, and threats. • Misspelling and threats were considered less trustworthy than financial and urgency indicators. • The presence of phishing indicators did not considerably affect the time spent looking at the rest of the e-mail. • The trustworthiness rating cannot be explained by the total time spent looking at phishing indicators.
[14]	Experiment, 25 participants (3 excluded)	• The best phishing e-mail could fool 40% of participants with a technical background. • Mainly, users looked at the body and header of an e-mail. • Knowledge and processing time are the two most important factors for identifying phishing e-mails.
[15]	Experiment, 23 participants	• The average detection error rate was 41.1%, in which 61 (30.5%) were false negatives, and 28 (21.4%) were false positives out of the 331 times the address bar was gazed. • Identification of phishing websites is improved by checking the address bar.
[16]	Experiment, 107 participants	• Experienced users attended and recognized more security-related information cues. • Situational information security awareness is not significantly impacted by agreeableness. • Instead, it is negatively influenced by contextual relevance and misplaced salience. • Salient design elements, such as logos and images divert attention from security cues more than plain text. • Users are more attentive to cues in security warnings, which activate pattern matching mechanisms. • Perceiving phishing as threatening generates a fear that indirectly but strongly invokes taking protective actions.
[17]	Case study , 160	• Users paid more attention to AOIs rather than uninformative and

	participants	distraction areas. • According to the average pupil diameter, users paid least attention to the sender, and most to the main e-mail content, followed by the salutation. • Persistent highlighting reduced attention spans on the main content.
[18]	User study, 20 participants	• Users' cognitive resources have a cap of around 100 characters when vetting a URL. • Users tend to believe that the presence of "www" in the domain name indicates the safety of a URL, and do not carefully parse the URL beyond that.
[19]	User study, unspecified	• Users who are more susceptible to phishing mainly focus less informative components; the e-mail content and images (if present). • For those users, the total number of gazes is generally lower. • Users who are less susceptible to phishing focus more on the sender's address and the URL (if present).
[20]	User study, 21 participants	• When evaluating the authenticity of a website, users only spend 6% of their time looking at security indicators. • On the other hand, 85% of their time is spent looking at website content. • A positive correlation is found between the time spent looking at security indicators and the correct identification of phishing websites.
[21]	Two experiments, 60 and 45 participants	• Users who followed the authorization dialogue approach could identify permissions better than others. • The former group of users had a significantly higher average number of eye-gaze fixations on the permission text than other group participants.
[22]	Experiment, 50 participants	• The phishing susceptibility prediction model (DSM) had a higher correct prediction rate (92.34%) than that for individual feature prediction. • Combining static and dynamic features, DSM is an effective predictor of users' susceptibility to phishing.
[23]	Experiment, 4 participants	• All users focused on "Emergency Earthquake Warning." • Users with high literacy gazed at the domain name of the e-mail address.
[24]	Experiment, 23 participants	• When only checking content, phishing recognition performance returned an average error rate of 32.4% compared to 13.5% when security indicators are also checked. • The accuracy of user susceptibility to phishing based on eye movement is 79.3%.
[25]	Experiment, 107 participants	• In 26% of all cases, participants clicked on enclosed links or downloaded attachments in phishing e-mails. • In 38% of all cases, participants deleted or archived phishing e-mails in the spam folder, whereas they reported them in only 8% of all cases. • Experience and attention to security cues enable identifying and handling phishing e-mails. • Salient elements, such as logos, images or buttons divert attention from security cues more than plain text.
[26]	Experiment, 36 participants	• 90% of users depend on the domain name of a website as a legitimacy indicator. • Website design influences user decision on the legitimacy of a website.
[27]	Experiment, 40	• Knowledge and awareness about phishing were insufficient for

	participants	cyber protection, as even knowledgeable participants had insecure behaviours. • Attentiveness helps reduce susceptibility to phishing attacks. • Insecure behaviors continue to increase the likelihood of falling victim to phishing attacks.
[28]	Experiment, 22 participants	• Eye gaze fixation agreed with task performance. • Highlighted domains attracted visual attention, but did not effectively protect against phishing.
[29]	Experiment, 25 participants	• Users do not spend enough time analyzing key phishing indicators. • Longer fixations on login forms and logos may have regarded them as better than real legitimacy indicators. • Users who look longer at the login field are likely to have lower accuracy. • Personality traits (e.g, high attention control) improves phishing detection accuracy.
[30]	Usability study, 60 participants	• The domain name was used the most to determine legitimacy. • Less than 20% checked the SSL/TLS indicator. • Simple design is not necessarily better in mitigating phishing.
[31]	Simulated experiment, 41 participants	• Context-based micro-training increases user awareness. • Less than 10% of users could identify all phishing e-mails correctly. • Less than 50% of users evaluated all phishing identifiers.
[32]	Experiment, 132 participants	• Users unconsciously pay less attention to previously seen warnings. • Such habituation effect quickly sets in and progresses with successive warning exposures.

4. DISCUSSION

4.1. Technical Attributes

While scanning phishing materials, participants have shown to have some ability of recognizing some features associated to fraudulence. Yet, the general absence of a statistically significant correlation between detection accuracy and gaze fixation on the entire phishing material makes it unclear whether these materials, which exploit heuristics and invoke a cognitive miser style of processing, are successfully achieving their purpose. Nonetheless, participants rated e-mails containing misspelling rated as less trustworthy than others, as misspelling is a more categorical factor than urgency or threat indicators, which are open to personal interpretation.

For URLs, users can only expend a finite budget of resources to classify legitimacy. If the required resources exceed the budget, users will not expend them. Although threshold depends on factors other than the URL length, this notion is expected to apply generally.

Since fixation and dwell times are the highest for e-mail senders and website address bars, it is inferred that addresses are perceived as helpful phishing indicators. However, a single AOI does not necessarily translate into sound phishing determinations. This can be proven by the improved performance for users who studied multiple AOIs. Specific content, namely that asking for credit card information, was most likely to be identified as illegitimate. It can be assumed that most users have heard about phishing through the typical warning of messages asking for credit card information. In addition, contextual relevance and misplaced salience negatively impact security awareness. When users face messages aligned with their work context, they pay less attention to security-related cues compared to when they are misaligned. As for salient design elements, they draw attention away from cues more than plain text.

4.2. Personal Attributes

Personal attributes, including experience, have shown to positively impact phishing detection. To demonstrate, users with past experience in web architecture, such as the ability to precisely interpret URLs, locks and page redirection, have demonstrated awareness by attending to a larger number of security-related information cues [35]. As such, it is inferred that experience allows the development of schemata [36] and identifying critical cues which enable pattern matching while forming awareness. On the other hand, other users seem to compensate for the lack of domain knowledge and experience by allowing more processing time to each e-mail or website. Comparing the average glance duration of both groups, it must be emphasized that the processing time for non-experts is a crucial factor.

An important factor which highly affects detection accuracy is attention control. Considered a personality trait [37], attention control has shown a high correlation with the ability to correctly detect phishing. It is characterized by pupil dilation [38], which provides an index of overall attentional effort, though it is time-locked to stimulus changes during attention.

Prior empirical studies have suggested mixed results on the association of personal attributes to phishing susceptibility. Yet, findings of this work agree with the majority of previous studies in terms of reporting insignificant correlations to agreeableness [39]. Therefore, a higher level of agreeableness does not translate to less attention to security-related cues.

Although domain knowledge, experience and attention control are key factors for mitigating phishing attacks [40], [41], it should be emphasized that they do not entirely guarantee user safety. Instead, risk awareness must be linked to a perceived vulnerability or a mitigation strategy, as perceived severity of consequences does not necessarily produce secure behavior.

4.3. Urgency and Threat Attributes

As for phishing indicators relating to urgency and threats, their immediate capture of human attention could be justified by survival information bias [42], in which humans prioritize processing information possibly related to their well-being. Security warnings have been shown to positively impact awareness by activating pattern matching mechanisms, which increase attentiveness to cues. Further, an indirect relationship between perceived threat and protection motivation suggests that perceiving phishing as threatening motivates users to take protective measures against phishing. Conversely, findings suggest that those who are aware of security-related cues are more confident in taking appropriate actions, thus exhibiting a higher perceived coping efficacy which positively influences protection motivation.

On the long term, the work in [32] presents a thorough study on habituation to visual stimuli, which demonstrates that habituation causes a steep decrease in attention after a few exposures. That is, it suggests that repeated exposure to security warnings may cause warnings to be physically seen, but not truly perceived by users. Specifically, gaze duration will decrease over successive viewings, and will decrease faster when viewing static warnings as compared to polymorphic warnings.

Taking these findings into account, it must be highlighted that computed detection accuracies in the studies are expected to be upper bounds on what users would achieve in practice, as additional safeguards in the artificial experimental setting would be removed.

5. IMPLICATIONS

Results demonstrate a number of fundamental points; they provide evidence that eye-tracking technology is useful in collecting gaze data on humans and phishing AOIs. Building upon this work provides more avenues for improving existing technology and increasing human awareness, all of which will be explored in this section.

5.1. User-Friendly URLs

From a technical standpoint, there exists no intrinsic security benefit to shortening a URL, beginning a domain name with www, or having a few special characters. In [20], although most users attempted at least occasionally to use the URL, they were not knowledgeable enough about URL structures to make informed decisions. For this reason, a more user-friendly URL bar should be developed. Specifically, domain names need to be more visually distinct to be effective security cues [43]. Alternatively, "breadcrumbs" could be used in browsers as in file managers to display the domain name more prominently, and users can view the whole URL by clicking on the URL bar. Since domain highlighting has not proven effectiveness, [16] recommends improving the design of indicators by changing the color, size or position to produce more salient cues for users.

5.2. Visual Aids for Browsing

The collected eye-tracking data can be useful in developing a gaze position indicator which informs the user when their gaze moves from one domain to another. That is, visualization could facilitate noticing changes even with less levels of attention. In [17], this data was used to develop a human-technical solution to guide user attention to the correct e-mail AOIs and therefore improve phishing detection accuracy. Nevertheless, the browser extension in [15] interacts with an eye-tracking device in order to develop satisfactory security behavior. By requiring users to look at the address bar before entering information, EyeBit checks whether users look at the address bar in browsers to improve security.

Real-time eye-gaze features can be used to automatically infer attentiveness states and assess the reliability of respective user response. Better yet, combining neural and ocular features will provide a robust detection system in which higher security measures will be achieved.

5.3. Embedded and Automated Authentication

Embedded authentication facilitates informing users about the legitimacy of a website. Yet, a potential implementation issue is the limited support for smartphones. Due to their constrained user interfaces by small screens, smartphone browsers often lack trustworthiness indicators. To solve this issue, it is recommended to implement a lightweight algorithm into smartphone browsers to deceptively detect phishing websites without user interaction. For instance, fake login credentials were used in [25] while simultaneously monitoring the destination server HTTP responses to authenticate a web page. Similarly, the UnPhishMe logic in [27] was implemented on a web browser to mitigate the exposure of login information to attackers, as well as eliminate zero-day and zero-hour phishing attacks in real-time.

5.4. Education and Training

The two most important factors in recognizing and, in return, mitigating phishing attacks are knowledge and attentiveness. At best, users should become experts to avoid falling victim for phishing. Through the assessment, comparison and improvement of training modules, training programs with heavy user involvement significantly impact user detection accuracy. For instance, educational materials and training strategies proposed by Merwe et al. in [42] compare phishing attacks with provided security service guidelines, and pinpoint weaknesses in the former if users adhere to the guidelines. Nonetheless, other training strategies were proposed in [44-46], and have proven effective in minimizing phishing susceptibility.

In [25], it was found that contextual relevance negatively impacts situational Information Security Awareness (ISA), which emphasizes the importance of tailoring phishing exercises to users and challenging employees with contextually relevant materials. On the other hand, training implementers must acknowledge the relevancy of each phishing material for trainees. To demonstrate, some employees may regularly interact with third-party groups, therefore increasing their exposure to phishing. In this case, they should acquire situational ISA by regularly matching AOI patterns with their mental library of what an AOI should look like to determine legitimacy.

To manage different abilities, difficulty levels of training sets should be personalized by varying the number of manipulated security cues to adhere to all trainees. One example is the implementation of EyeBit [15], which encouraged user attentiveness by tailoring training materials according to experience levels. For more experienced individuals, the variation of more difficult materials enhances their mental models and counters possible stereotypes which may have developed through repeated exposure. Conversely, less experienced individuals may benefit more from simpler materials of fewer manipulated cues to initially develop a mental library of prototypical phishing materials.

6. Limitations of the Literature

As seen in Table 5, relatively small sample sizes were used in some studies. Compared to previous eye-tracking studies [47-49], this is not atypical. However, a small sample size is insufficient to investigate individual variability in how well eye-tracking estimates the ability to spot phishing attacks. Moreover, some eye-tracking data was excluded due to low validity scores arising from measurement devices and participant imprudence. For instance, sudden head, neck and/or face movements interfered with produced results. Consequently, reduced sample sizes may cause overfitting problems. Nevertheless, such problem can be suppressed by using head-mount eye-tracking devices or retaking measurements, if feasible. Also, some samples were of predominantly one gender. Although no evidence of gender differences in eye movements can be found [50], consistent research on the role of gender in phishing susceptibility remains a necessity [51]. Nonetheless, recruiting a more diverse sample and adopting the Bayesian optimization feedback loop [52], which adapts to unconsidered user groups, may clarify whether certain types of phishing are of more impact on different demographic groups.

The second limitation is the artificial setting of the experiments causing participation bias. Participants were explicitly informed that they are to spot phishing e-mails and/or websites. As demonstrated by [53], phishing detection accuracy may be higher when participants are aware in advance of the detection task. Therefore, results are expected to demonstrate an upper-bound on users’ ability to correctly identify phishing, which is concerning given that detection accuracy was generally low. As such, a better experimental design would be to process phishing content as a secondary task, where phishing content is randomly spread and participants are monitored to check if they would share sensitive data.

The third limitation is the utilization of online sources for the majority of phishing materials. Despite having an element of realism, some content was not ideal for experimental designs due to conflation of different phishing techniques, such as the combination of threat and urgency. Additionally, some content was presented to participants in the form of screenshots. While this method kept participants focused on the tasks, they were unable to interact with presented materials as they would in a real-life setting.

Another limitation is the classification of phishing content into AOIs, which may lead to correct detection but for completely wrong reasons. To modify this classification, AOIs could be formed only where phishing content can also be detected, and user perception as well as time taken to find these explicit recognition features can be studied. Moreover, given that some AOIs were relatively small, the error margin may have impacted the results, such as the recognition of the address bar in [15] by EyeBit. On the other hand, some used larger fonts and displayed URLs over multiple lines, which may have affected visual behavior and responses. A possible solution in this case is pattern matching in a digitized image, or estimating the position from the top-left browser corner. In both cases, it will be mandatory to adjust for each participant. Furthermore, it is to be noted that dwell time on an AOI does not necessarily reflect the level of understanding of a security cue. Conversely, a short glance duration does not necessarily indicate missing that element. In other words, it is possible to interpret the collected data differently.

Analyzing eye-tracking data is an objective step in the attempt to reflect and assess information security awareness. Although detection accuracy has generally improved compared to the past, it is unclear whether such improvement can be traced back to improved interfaces as opposed to increased user threat awareness. Considering these limitations, it is necessary to generate deeper and more valuable insights in order to form a comprehensive understanding and produce more results of high confidence.

7. CONCLUSIONS

In this work, 20 empirical studies have been pooled to examine phishing susceptibility through the lens of eye-tracking. Results provided empirical evidence that a user of a higher detection accuracy is characterized by higher attention control; spending more time looking at an AOI. Eye-tracking behavior has also shown that other attributes, namely technical background, domain knowledge, experience, training, and risk perception contribute to mitigating these attacks. In contrast, derived gaze position metrics, including TTFF, entry time and entry sequence data yielded inconclusive results regarding the impact on susceptibility to phishing attacks. It must be stressed that establishing user awareness has become of paramount importance, as one manipulated user could cause a catastrophic loss on both a personal and business infrastructural level. Thus, understanding how users determine the legitimacy of online content is a crucial step into developing usable security cues and training programs to mitigate phishing.

ACKNOWLEDGEMENTS

I would like to thank Dr. Shi Cao at the University of Waterloo for providing insight and knowledge into human factors testing, which steered me through this research. Dr. Shi Cao provided continuous encouragement, guidance and feedback and was always enthusiastic to assist in any way throughout the course.

REFERENCES

[1] Lee, S.hyun. & Kim Mi Na, (2008) "This is my paper", ABC Transactions on ECE, Vol. 10, No. 5, pp120-122.

[2] Gizem, Aksahya & Ayese, Ozcan (2009) Coomunications & Networks, Network Books, ABC Publishers.

[3] Slandau, "Phishing Attack Statistics 2022," CyberTalk, 05-Apr-2022. [Online]. Available: https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/#:~:text=In%202021%2C%2083%25%20of%20organizations,s%20doubled%20since%20early%202020.

[4] M. Lukings and A. H. Lashkari, Understanding Cybersecurity Law and Digital Privacy: A Common Law Perspective. Cham: Springer International Publishing AG, 2022.

[5] R. Banerjee, Corporate Frauds Business Crimes Now Bigger, Broader, Bolder. SAGE Publications, 2022.

[6] "FBI: Internet Crime Report 2021," Internet Crime Complaint Center, pp. 22, 2022.

[7] 2021 Cyber Security Threat Trends: Phishing, Crypto Top the List. Cisco Umbrella. [Online]. Available: https://cloudmanaged.ca/wp-content/uploads/2021/09/2021-cyber-security-threat-trends-phishing-crypto-top-the-list.pdf.

[8] M. K. Eckstein, B. Guerra-Carrillo, A. T. Miller Singley, and S. A. Bunge, "Beyond Eye Gaze: What Else Can Eyetracking Reveal about Cognition and Cognitive Development?," Developmental Cognitive Neuroscience, vol. 25, pp. 69–91, 2017.

[9] D. E. Hannula, "Worth a Glance: Using Eye Movements to Investigate the Cognitive Neuroscience of Memory," in Human Neuroscience, vol. 4, 2010.

[10] H. J. Green, P. Lemaire, and S. Dufau, "Eye Movement Correlates of Younger and Older Adults' Strategies for Complex Addition," Acta Psychologica, vol. 125, no. 3, pp. 257–278, 2007.

[11] K. Rayner, "Eye Movements in Reading and Information Processing: 20 Years of Research," Psychological Bulletin, vol. 124, no. 3, pp. 372–422, 1998.

[12] E. R. Grant and M. Spivey, "Eye Movements and Problem Solving: Guiding Attention Guides Thought," Psychological Science, vol. 14, pp. 462–466, Oct. 2003.

[13] B. Rehder and A. B. Hoffman, "Eyetracking and Selective Attention in Category Learning," Cognitive Psychology, vol. 51, no. 1, pp. 1–41, 2005.

[14] T. Whalen and K. Inkpen, "Gathering Evidence: Use of Visual Security Cues in Web Browsers," Proceedings of the Graphics Interface 2005 Conference, January 2005.

[15] J. McAlaney and P. J. Hills, "Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking," Frontiers in Psychology, vol. 11, 2020.

[16] K. Pfeffel, P. Ulsamer, and N. H. Mu¨ller, "Where the User Does Look When Reading Phishing Mails– An Eye-Tracking Study," Learning and Collaboration Technologies. Designing Learning Experiences, pp. 277–287, 2019.

[17] D. Miyamoto, T. Iimura, G. Blanc, H. Tazaki, and Y. Kadobayashi, "EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits," 2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), 2014.

[18] L. Jaeger and A. Eckhardt, "Eyes Wide Open: The Role of Situational Information Security Awareness for Security-Related Behaviour," Information Systems Journal, vol. 31, no. 3, pp. 429–472, 2020.

[19] L. Huang, S. Jia, E. Balcetis, and Q. Zhu, "ADVERT: An Adaptive and Data-Driven Attention Enhancement Mechanism for Phishing Prevention," IEEE Transactions on Information Forensics and Security, pp. 1–1, 2022.

[20] N. Ramkumar, V. Kothari, C. Mills, R. Koppel, J. Blythe, S. Smith, and A. L. Kun, "Eyes on URLs: Relating Visual Behavior to Safety Decisions," ACM Symposium on Eye Tracking Research and Applications, 2020.

[21] "Eye-Tracking Phishing E-mails," Objective Experience SG Blog, 09-Nov-2017. [Online]. Available: https://eyetrackinginasia.wordpress.com/2017/11/09/eye-tracking-phishing-e-mails/.

[22] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why Phishing Still Works: User Strategies for Combating Phishing Attacks," International Journal of Human-Computer Studies, vol. 82, pp. 69–82, 2015.

[23] Y. Javed and M. Shehab, “Look Before You Authorize: Using Eye-Tracking to Enforce User Attention towards Application Permissions,” Proceedings on Privacy Enhancing Technologies, vol. 2017, no. 2, pp. 23–37, 2017.

[24] R. Yang, K. Zheng, B. Wu, C. Wu, and X. Wang, “Prediction of Phishing Susceptibility Based on a Combination of Static and Dynamic Features,” Mathematical Problems in Engineering, vol. 2022, pp. 1–10, 2022.

[25] T. Matsuda, R. Ushigome, M. Sonoda, H. Satoh, T. Hanada, N. Kanahama, M. Eto, H. Ishikawa, K. Ikeda, and D. Katoh, “Investigation and User’s Web Search Skill Evaluation for Eye and Mouse Movement in Phishing of Short Message,” Advances in Intelligent Systems and Computing, pp. 131–136, 2019.

[26] D. Miyamoto, G. Blanc, and Y. Kadobayashi, “Eye Can Tell: On the Correlation Between Eye Movement and Phishing Identification,” Neural Information Processing, pp. 223–232, 2015.

[27] L. Jäger and A. Eckhardt, “Phish Me If You Can: Insights from an Eye- Tracking Experiment,” OPUS 4. [Online]. Available: http://publikationen.ub.uni-frankfurt.de/frontdoor/index/index/year/2021/docId/61421.

[28] A. Darwish and E. Bataineh, “Eye Tracking Analysis of Browser Security Indicators,” 2012 International Conference on Computer Systems and Industrial Informatics, 2012.

[29] J. D. Ndibwile, E. T. Luhanga, D. Fall, D. Miyamoto, G. Blanc, and Y. Kadobayashi, “An Empirical Approach to Phishing Countermeasures Through Smart Glasses and Validation Agents,” IEEE Access, vol. 7, pp. 130758–130771, 2019.

[30] A. Xiong, R. W. Proctor, W. Yang, and N. Li, “Is Domain Highlighting Actually Helpful in Identifying Phishing Web Pages?,” Human Factors: The Journal of the Human Factors and Ergonomics Society, vol. 59, no. 4, pp. 640–660, 2017.

[31] A. Neupane, M. L. Rahman, N. Saxena, and L. Hirshfield, “A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings,” Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015.

[32] A. Darwish and F. Aloul, “Impact of Page Design Factor on Cyber Security,” 2014.

[33] J. Kävrestad, A. Hagberg, M. Nohlberg, J. Rambusch, R. Roos, and S. Furnell, “Evaluation of Contextual and Game-Based Training for Phishing Detection,” Future Internet, vol. 14, no. 4, p. 104, 2022.

[34] B. B. Anderson, J. L. Jenkins, A. Vance, C. B. Kirwan, and D. Eargle, “Your Memory is Working Against You: How Eye Tracking and Memory Explain Habituation to Security Warnings,” Decision Support Systems, vol. 92, pp. 3–13, 2016.

[35] “Phishing: Spot and Report Scam Emails, Texts, Websites and Calls,” National Cyber Security Centre, 26-Nov-2021. [Online]. Available: https://www.ncsc.gov.uk/guidance/suspicious-email-actions.

[36] A. T. Duchowski, Eye Tracking Methodology: Theory and Practice. Cham: Springer, 2017.

[37] “The Role of a Schema in Psychology,” The Role of a Schema in Psychology - Simply Psychology. [Online]. Available: https://www.simplypsychology.org/what-is-a-schema.html.

[38] J. S. Nairne, “Adaptive Memory: Evolutionary Constraints on Remembering,” Psychology of Learning and Motivation, pp. 1–32, 2010.

[39] K. Kaspar and P. König, “Emotions and Personality Traits as High-Level Factors in Visual Attention: A Review,” Frontiers in Human Neuroscience, vol. 6, 2012.

[40] T. Sommestad and H. Karlzén, “A Meta-Analysis of Field Experiments on Phishing Susceptibility,” 2019 APWG Symposium on Electronic Crime Research (eCrime), 2019, pp. 1-14, doi: 10.1109/eCrime47957.2019.9037502.

[41] H. van Steenbergen, G. P. Band, and B. Hommel, “Threat but not Arousal Narrows Attention: Evidence from Pupil Dilation and Saccade Control,” Frontiers in Psychology, vol. 2, 2011.

[42] R. Dhamija, J. D. Tygar, and M. Hearst, “Why Phishing Works,” Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2006.

[43] D. Harley and A. Lee, “Phish Phodder: Is User Education Helping or Hindering?” in Proceedings of the Virus Bulletin Conference, 2007, pp. 1–7.

[44] A. Van der Merwe, M. Loock, and M. Dabrowski, “Characteristics and Responsibilities Involved in a Phishing Attack,” in Proceedings of the 4th International Symposium on Information and Communication Technologies, Jan. 2005.

[45] M. Seckler, S. Heinz, S. Forde, A. N. Tuch, and K. Opwis, “Trust and Distrust on the Web: User Experiences and Website Characteristics,” Computers in Human Behavior, vol. 45, pp. 39–50, 2015.

[46] O. A. Zielinska, R. Tembe, K. W. Hong, X. Ge, E. Murphy-Hill, and C. B. Mayhorn, “One Phish, Two Phish, How to Avoid the Internet Phish,” Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 58, no. 1, pp. 1466–1470, 2014.

[47] Z. A. Wen, Z. Lin, R. Chen, and E. Andersen, “What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game,” Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019.

[48] C. Nguyen, M. Jensen, and E. Day, “Learning Not to Take the Bait: A Longitudinal Examination of Digital Training Methods and Overlearning on Phishing Susceptibility,” European Journal of Information Systems, pp. 1–25, 2021.

[49] J. J. Tecce, J. Gips, C. P. Olivieri, L. J. Pok, and M. R. Consiglio, “Eye Movement Control of Computer Functions,” International Journal of Psychophysiology, vol. 29, no. 3, pp. 319–325, 1998.

[50] M. Libben and D. A. Titone, “Bilingual Lexical Access in Context: Evidence from Eye Movements During Reading,” PsycEXTRA Dataset, 2007.

[51] W. Choi, M. W. Lowder, F. Ferreira, T. Y. Swaab, and J. M. Henderson, “Effects of Word Predictability and Preview Lexicality on Eye Movements During Reading: A Comparison Between Young and Older Adults,” Psychology and Aging, vol. 32, no. 3, pp. 232–242, 2017.

[52] C. Klein, C. Klein, and U. Ettinger, Eye Movement Research: An Introduction to its Scientific Foundations and Applications. Cham, Switzerland: Springer, 2019.

[53] S. Kleitman, M. K. Law, and J. Kay, “It’s the Deceiver and the Receiver: Individual Differences in Phishing Susceptibility and False Positives with Item Profiling,” PLoS ONE, vol. 13, no. 10, 2018.

[54] F. Archetti, Bayesian Optimization and Data Science. Springer International Publishing, 2019.

[55] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, “The Design of Phishing Studies: Challenges for Researchers,” Computers Security, vol. 52, pp. 194–206, 2015.

AUTHORS

Noon Hussein was born in Edmonton, AB, Canada in 1999 to an immigrant Sudanese family. She received her BSc in Electrical Engineering from Qatar University in 2021, and is currently pursuing her MASc in Pattern Analysis and Machine Intelligence (PAMI) at the University of Waterloo, ON, Canada. Her research interests include IoT, systems design, cybersecurity and engineering education.