POSTER: Cybersecurity Awareness Education: Just as Useful for Technical Users

Daniel Köhler[*,1][0000−0003−3121−3888], Michael Büßemeyer[1], and Christoph Meinel[1]

Hasso Plattner Institute, University of Potsdam, Potsdam, Germany
daniel.koehler@hpi.de
michael.buessemeyer@student.hpi.de

Abstract. Cybersecurity education is often perceived as necessary particularly for laypersons, as experts in the field are usually expected to be aware of the risks posed by human-centered attacks such as phishing. In a lab study with 48 participants from IT-related study programs, we studied their phishing investigation behavior using eye trackers across three email classification sessions. Between the first two sessions, participants received additional training on detecting phishing attacks. The third session, one week later served to measure retention of performance. Exposure to the teaching material particularly showed to decrease investigation time required for the classification. Further, it helped participants focus on the important indicators inside the phishing emails.

Keywords: Phishing · Education · Experts · Eye Tracking

1 Introduction

Cybersecurity attacks are still a dominant part of everyday life. With increased digital exposure, more and more people become potential targets for cybercriminals. Phishing, a threat from the social engineering category, has become a significant threat to people, having been used as a vector of initial access in more than 90% of data breaches as reported by Cisco [3].

The threat of email phishing can generally be accounted for by either technical controls such as email filters and sandboxes or by employing organizational measures such as people's education. Educational measures for phishing have been of great interest since the early years of phishing research. Much relevant work has been pursued by authors such as *Kumaraguru et al.* who investigated (game-based) educational measures to collect insights on participant perception and recall of phishing education [6, 7]. Further significant work has been aggregated by various researchers investigating which cues in emails particularly resonate with users and how users behave around phishing emails [9, 4].

Various previous publications, as analyzed in the comparative literature review by *Jampen et al.* [5] point out that the technicality of a target impacts their

[*] Corresponding Author.

Published in ACNS 2024 proceedings by Springer.
DOI: 10.1007/978-3-031-61489-7_15

susceptibility to fall victim to a phishing attack. Therefore, phishing education is often aimed at laypersons to get them en-par with their more technically advanced peers to achieve an appropriate level of protection amongst, for example, employees in a company.

Our manuscript provides a preliminary insight into an in-lab study with 48 rather technical participants, each categorizing a total of 30 emails for being phishing or legitimate across three study sessions. During the sessions, participant behavior was tracked by an eye tracker to ensure that the categorization performance and the decision process could be analyzed. From the data collected during our study, we present one preliminary contribution:

While educational material has not increased the classification performance of participants, it reduced the time required for the classification activity and increased the relative time of focus on phishing indicators inside the emails.

2 Methodology

Our in-lab study featured a multi-stage design as presented in Figure 1. In a total of two sessions per participant, participants performed a three email classification tasks. In-between, they were exposed to different teaching materials[1] and a break of one week to measure retention. During the conceptualization of our study, we prepared three sets of emails with ten emails each. To ensure an internally valid study design, these were distributed among participants so that each sequence of email sets was studied with eight participants (48 participants and six variations of sequence of the email sets). Further, we designed our emails to be of similar difficulty across the three sets. To achieve this, each email set contained six phishing emails of differing difficulty (2 easy, 2 medium, 2 difficult), and four legitimate emails. Emails were designed based on vectors reported by previous research such as being *Loss-*, or *Reward-Based* [2], containing *images and logos* [10], a *personal salutation* and targeting psychological vectors such as *urgency* or *fear* [8].

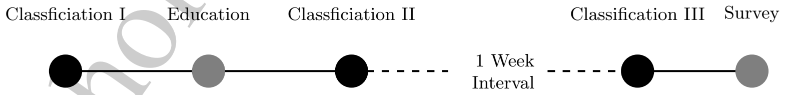


Fig. 1: Overview of the study design featuring three email classification sessions, intervened with an education session and a one-week study interception.

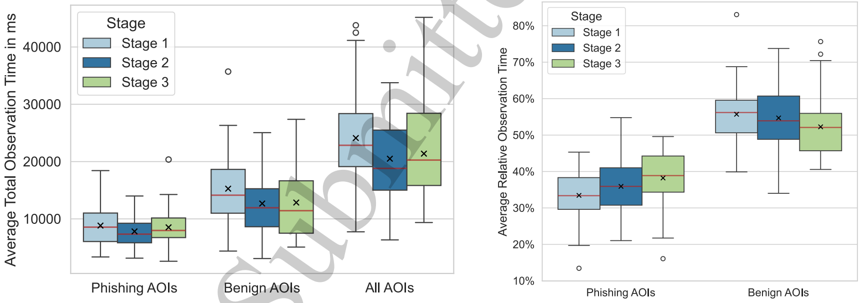
During the classification tasks, participants were recorded by an eye tracker, which allowed later analysis of behavior on top of an analysis of classification

[1] The analysis of this work towards the impact of the different types of teaching materials has not yet been completed. This poster hence omits the differentiation between the four styles of teaching material and solely presents overarching results.

performance. Our participants were students recruited from the Bachelor and Master programs in Digital Engineering at the Hasso Plattner Institute. Therefore, all participants have a relatively high affinity towards IT systems. In the survey, participants further reported their self-perceived cybersecurity knowledge on a scale from 1 (*No Knowledge*) to 5 (*Expert Knowledge*). Most participants rated their knowledge as level 2 (N=20) or level 3 (N=17), thereby confirming the assumption of a relatively coherent skill level among participants.

3 Study Results

Across the three classification tasks in the three stages of the study, the performance in terms of correct classifications did not significantly change. The performance across all the stages averaged at 84.01% correct classifications ($P_{S1} = 84.38\%, P_{S2} = 83.75\%, P_{S3} = 83.91\%$). As the classification performance was neither affected by the study material nor by the interval of one week between stages two and three, we investigated other behavior measures.



(a) **Absolute** observation time

(b) **Relative** observation time

Fig. 2: Email viewtime throughout the different stages of the study. Aggregated average viewtimes for phishing and beneign AOIs in phishing emails.

One measure we could investigate based on the used eye tracker was the time a participant spent on their classification tasks. Figure 2a presents an overview of averaged **absolute email observation** times. We categorized all areas of interest (AOIs) inside the emails into either phishing or benign. While viewing phishing AOIs should induce suspiciousness, viewing benign areas should increase the trustworthiness of an email. As Figure 2a shows, after consuming the teaching material, the absolute view time of emails increases in the test for retention in stage three. We could not observe statistically significant differences in the absolute view times of the phishing or benign indicators.

Due to the change in overall email viewtime, Figure 2b presents the averaged **relative viewtime** of phishing and benign indicators. Visually observable is that throughout the three stages, even after the one-week intervention, the average relative time spent investigating phishing indicators increases from 33.44% in stage one to 38.22% in stage three. This difference is significant as confirmed with a t-test with $p = 0.0018$, assuming $\alpha = 0.05$ as threshold for significance.

Figure 3 presents additional detailed information on the phishing indicators viewed and investigated by participants. We observe the consistent increase of relative viewtime for the indicators surrounding the *sender address (suspicious part)* and *domain*. Therefore, participants now focus more on the email addresses and corresponding domains used in the phishing emails. Such behavior can properly help detect various forms of sender obfuscation currently observed in the wild, such as attackers using additional top level domains to obfuscate their phishing attempts (e.g., *amazon.supportsite.com* instead of *amazon.com* to imitate a supposed helpdesk).

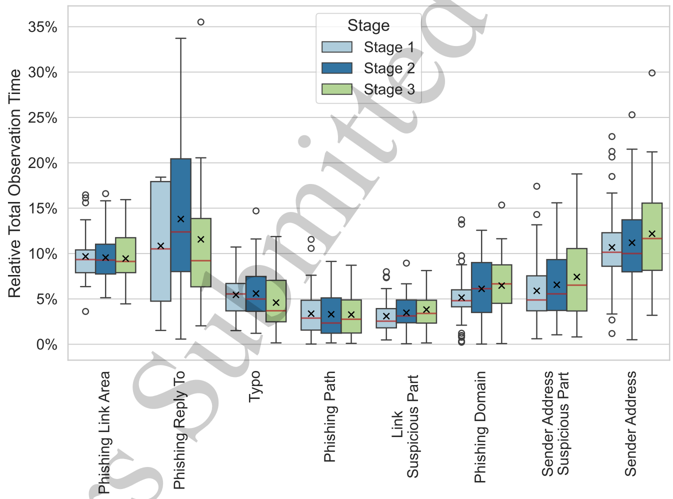


Fig. 3: Overview of the averaged relative viewtime of phishing and benign AOIs.

4 Discussion and Conclusion

This work shall open up discussions on whom to target with phishing education. Further, we appreciate discussion on study designs that would allow a more appropriate attribution of the observed effect to the educational material instead of the repetition of the classification exercise.

The preliminary results of our study show that while educational content did not improve classification performance of participants with high IT affinity, it improved how they classify emails. The data indicates that participants take overall less time to classify emails. The educational material has highlighted common measures to identify phishing and the analysis has shown that participants focus more on phishing indicators. They *lose* less time during email analysis to investigating benign indicators and spend their time more efficiently.

Author Contributions

Contributions according to the CRediT Framework [1]: **Daniel Köhler:** Writing, Conceptualization, Supervision, Project Administration, Investigation **Michael Büßemeyer:** Methodology, Software, Formal Analysis, Data Curation, Visualization **Christoph Meinel:** Funding Acquisition

References

1. Allen, L., O'Connell, A., Kiermer, V.: How can we ensure visibility and diversity in research contributions? How the Contributor Role Taxonomy (CRediT) is helping the shift from authorship to contributorship. Learned Publishing **32**(1), 71–74 (Jan 2019). https://doi.org/10.1002/leap.1210
2. Baryshevtsev, M., McGlynn, J.: Persuasive Appeals Predict Credibility Judgments of Phishing Messages. Cyberpsychology, Behavior, and Social Networking **23**(5), 297–302 (May 2020). https://doi.org/10.1089/cyber.2019.0592
3. Cisco Umbrella: Cybersecurity threat trends: phishing, crypto top the list (2021), https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list
4. Furnell, S.: Phishing: can we spot the signs? Computer Fraud & Security **2007**(3), 10–15 (Mar 2007). https://doi.org/10.1016/S1361-3723(07)70035-0
5. Jampen, D., Gür, G., Sutter, T., Tellenbach, B.: Don't click: towards an effective anti-phishing training. A comparative literature review. Human-centric Computing and Information Sciences **10** (2020). https://doi.org/10.1186/s13673-020-00237-7
6. Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L.F., Hong, J.: Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. In: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit. pp. 70–81 (2007)
7. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., Hong, J.: Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology **10**(2), 1–31 (May 2010). https://doi.org/10.1145/1754393.1754396
8. McAlaney, J., Hills, P.J.: Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking. Frontiers in Psychology **11** (2020), https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01756
9. Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., Jerram, C.: Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails. In: Janczewski, L.J., Wolfe, H.B., Shenoi, S. (eds.) Security and Privacy Protection in Information Processing Systems. pp. 366–378. IFIP Advances in Information and Communication Technology, Springer, Berlin, Heidelberg (2013)
10. Williams, E.J., Polage, D.: How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. Behaviour & Information Technology **38**(2), 184–197 (Feb 2019). https://doi.org/10.1080/0144929X.2018.1519599