

“I Know What They Are Trying...!” – The Influence of Awareness of Persuasive Strategy Usage on Phishing Email Recognition Accuracy

Asal Hojjati^{1,2} and Jaap Ham^{2,*}

¹ Industrial Engineering Department, Sharif University of Technology, Tehran, Iran

² Human-Technology Interaction, Eindhoven University of Technology, Eindhoven, The Netherlands

1. Introduction

Phishing is a socially engineered threat that acquire sensitive information from people through online devices [1]. This attack has caused countless security breaches during the past few years, occurring more frequently and diversifying [2]. The success of phishing attacks depends mostly on human failure: Phishers take advantage of the user's trust in technology [3].

Recent studies trained people in identifying phishing emails (e.g., by their visual characteristics) using earlier phishing emails examples. In some cases, these trainings were successful ([1], [4]). Still, we argue that in the long run the effect of such training will be limited because phishers rapidly change and evolve their email design.

Independent from their design, we know that phishing emails have a universal characteristic: they attempt to influence the user to perform certain behaviors (e.g., clicking on a URL or logging in a website). For that, phishers use certain influencing strategies. We argue that if people would be able to recognize the influencing strategies used by this technology and beware of these strategies and technologies using them, we could help people defend themselves against phishing emails, independent of their design.

Earlier research, to our knowledge, has not investigated how to stimulate people to recognize phishing attacks that use these influencing strategies. Therefore, the aim of this study is to answer the following question: *What is the influence of training people to recognize technology using certain influencing strategies on compliance behavior?*

2. Method

Participants were randomly assigned to a 2 (training: identifying influencing strategies vs. not aimed at identifying influencing strategies) x 2 (influencing strategies in email: yes vs. no) mixed design, in which training was manipulated between participants, and influencing strategies in email was manipulated within participants.

A 2x2 F-test power analysis suggested our study would need 130 participants (power 0.90, effect size of 0.25, and $\alpha = 0.05$). Overall, 150 individuals participated in this study. Data were collected through an online survey. Half of the participants viewed a 2 minute training video about influencing strategies, and the other half a training video on the evolution of emails. Then, both groups filled out a survey which contained six email texts. Half of these emails contained various influencing strategies and half contained very few. Each email was followed by five

Persuasive 2023, Adjunct Proceedings of the 18th International Conference on Persuasive Technology, April 19–21, 2023, Eindhoven, The Netherlands

*Corresponding author.

✉ j.r.c.ham@tue.nl (J. Ham)

ORCID 0000-0003-1703-5165 (J. Ham)



© 2023 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).



CEUR Workshop Proceedings (CEUR-WS.org)

questions assessing the users' intention towards a phishing email, and their (spontaneous) identification of influencing strategies used in the email.

3. Results

Results provided no evidence supporting our expectation (H1) that participants who had been trained in identifying influencing strategies would intend to click on less links in emails that contain influencing strategies compared to the untrained group, which we tested using a chi-square test, $p > .05$. Supporting our second hypothesis (H2), results did provide evidence that participants who had been trained in identifying influencing strategies identified manipulation better than the untrained participants. Also, in support of our third hypothesis (H3), results showed that (a user) identifying manipulation had a negative correlation with the user's compliance intention, as indicated by a strong negative correlation.

4. Conclusion

Although the current results provided no evidence that participants who viewed our training video intended to click less on links than participants in the control group, results did provide evidence that participants who had been trained in identifying influencing strategies perceived manipulation better than the untrained participants, and we found a strong negative correlation between a user's identification of influencing strategies and intention of clicking on the link. This finding suggested that participants who recognized the use of manipulation techniques in emails, may avoid clicking on the links and may have a better chance of keeping away from malicious phishing attacks. These results can help develop better countermeasures against phishing attacks and more powerful ways of training against these attacks, and could also be helpful against any other form of manipulation.

References

- [1] Suganya, V. (2016). A Review on Phishing Attacks and Various Anti Phishing Techniques. *International Journal of Computer Applications*, 139.
- [2] Stefan A. Robila, James W. Ragucci. (2006). *Don't be a Phish: Steps in User Education*. Association for Computing Machinery.
- [3] I. Vayansky, S. Kumar. (2018). Phishing—challenges and solutions. *Computer*, 1, 15-20.
- [4] Ponnuram Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge. (2007, April). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. *Proceedings of the SIGCHI conference*