Clickthrough Testing for Real-World Phishing Simulations

Marc J. Dupuis*
marcjd@uw.edu
University of Washington
Bothell, Washington

Samantha Smith
ses1348@uw.edu
University of Washington
Bothell, Washington

ABSTRACT

In this paper, we begin by discussing the challenges associated with phishing email simulations. In part, we note how challenging it is to achieve realism in such a simulation and what this may mean for the results obtained. Next, we detail a real-world phishing simulation that targeted participants involved in an unrelated research project.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; *Privacy protections*; **Phishing**.

KEYWORDS

phishing, real-world experiment, social engineering, law, ethics

1 INTRODUCTION

The continued success of social engineering attacks is perhaps most evident in the use of and response to phishing emails. Despite the relatively long history of studying phishing and attempts to mitigate its effectiveness (e.g., [5]), it remains a significant challenge and threat for end users, including to their personal information [2]. There are many challenges associated with phishing email simulations. In particular, it can be incredibly difficult to achieve *realism* in such a simulation. This has implications for the results obtained and any inferences that can be reasonably drawn. A realistic looking phishing email will mimic what individuals would typically receive from an organization or other entity for which they have a prior relationship. The problem is that emulating such an email inherently means using the name, likeness, and images associated with that entity; this presents legal challenges for the campaign.

2 RELATED WORK

Previous studies have used a variety of experiments to test user susceptibility. These experiments have varied between extremely controlled lab conditions [4], in which participants were fully aware of the nature of the study to uninformed participants receiving phishing emails and being notified and surveyed later [3]. The first type of study frequently suffers from the Hawthorne effect, as being aware that a study is based on phishing alter the way in which participants would otherwise behave.

3 METHOD

IRB approval was obtained prior to engaging in the phishing experiment. Due to the subterfuge involved in collecting data in a real-world scenario, we do not attempt to gain a user's information in any way. Participant information used in this experiment came from an unrelated study for which they were recruited. To track emails, each participant was assigned a random ID, which was appended to the URLs in the email. Then, the usage statistics were taken from the domain, and filtered to get the events. These were then re-attributed to the user with the relevant ID.

4 RESULTS

Of the 146 participants that were sent the email, only 16 clicked on the phishing link. Overall, 11.0% of the participants were successfully phished, which includes 5.7% of participants that identify as female and 19.3% of participants that identify as male. We conducted a chi-square test to determine if there was a significant difference based on gender and found that gender was related to the propensity to click on this phishing email, $\chi^2(2, \mathrm{N} = 146) = 6.73$, $p < .05$.

5 DISCUSSION

Ultimately, while we did receive data from our attempts, the use of real-world phishing exercises is very difficult. The struggle of bypassing built-in phishing detectors makes this form of research a Sisyphean endeavor. There are reasonable arguments that can be made related to the ethical issues involved in conducting phishing email experiments; these discussions should continue. However, the end goal of this research and similar research being done by others is to minimize the success with which actual phishing emails from real-world adversaries have in manipulating individuals to perform an action and/or disclose confidential information. In this limited experiment, our results suggest that individuals continue to click on links in phishing emails in relatively high numbers. Additional efforts in cybersecurity education are needed at all levels of education, including college [1].

REFERENCES

[1] M. Dupuis. Cyber security for everyone: An introductory course for non-technical majors. *Journal of Cybersecurity Education, Research, and Practice*, 2017(1, Article 3), 2017.

[2] M. Dupuis and R. Crossler. The compromise of one's personal information: Trait affect as an antecedent in explaining the behavior of individuals. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, page 4841–4850. IEEE, 2019.

[3] B. Harrison, E. Svetieva, and A. Vishwanath. Individual processing of phishing emails. *Online Information Review*, 40:265–281, Apr. 2016.

[4] S. Kleitman. It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling, Oct. 2018.

[5] R. C. Miller and M. Wu. *Fighting Phishing at the User Interface*, page 275–292. O'Reilly, 2005.

*Both authors contributed equally to this research.

SIGITE '20, October 7–9, 2020, Virtual Event, USA

ACM ISBN 978-1-4503-7045-5/20/10.
https://doi.org/10.1145/3368308.3415443