The Persuasive Phish: Examining the Social Psychological Principles Hidden in Phishing Emails

Olga Zielinska, Allaire Welk, and Christopher B. Mayhorn
Department of Psychology
North Carolina State University
Raleigh, NC
{oazielin, akwelk, cbmayhor}@ncsu.edu

Emerson Murphy-Hill
Department of Computer Science
North Carolina State University
Raleigh, NC
emerson@csc.ncsu.edu

ABSTRACT

Phishing is a social engineering tactic used to trick people into revealing personal information [Zielinska, Tembe, Hong, Ge, Murphy-Hill, & Mayhorn 2014]. As phishing emails continue to infiltrate users' mailboxes, what social engineering techniques are the phishers using to successfully persuade victims into releasing sensitive information?

Cialdini's [2007] six principles of persuasion (authority, social proof, liking/similarity, commitment/consistency, scarcity, and reciprocation) have been linked to elements of phishing emails [Akbar 2014; Ferreira, & Lenzini 2015]; however, the findings have been conflicting. Authority and scarcity were found as the most common persuasion principles in 207 emails obtained from a Netherlands database [Akbar 2014], while liking/similarity was the most common principle in 52 personal emails available in Luxemborg and England [Ferreira et al. 2015]. The purpose of this study was to examine the persuasion principles present in emails available in the United States over a period of five years.

Two reviewers assessed eight hundred eighty-seven phishing emails from Arizona State University, Brown University, and Cornell University for Cialdini's six principles of persuasion. Each email was evaluated using a questionnaire adapted from the Ferreira et al. [2015] study. There was an average agreement of 87% per item between the two raters.

Spearman's Rho correlations were used to compare email characteristics over time. During the five year period under consideration (2010-2015), the persuasion principles of commitment/consistency and scarcity have increased over time, while the principles of reciprocation and social proof have decreased over time. Authority and liking/similarity revealed mixed results with certain characteristics increasing and others decreasing.

The commitment/consistency principle could be seen in the increase of emails referring to elements outside the email to look more reliable, such as Google Docs or Adobe Reader ($r_s(850) = .12$, $p = .001$), while the scarcity principle could be seen in urgent elements that could encourage users to act quickly and may have had success in eliciting a response from users ($r_s(850) = .09$, $p = .01$). Reciprocation elements, such as a requested reply, decreased over time ($r_s(850) = -.12$, $p = .001$). Additionally, the social proof principle present in emails by referring to actions performed by other users also decreased ($r_s(850) = -.10$, $p = .01$).

Two persuasion principles exhibited both an increase and decrease in their presence in emails over time: authority and liking/similarity. These principles could increase phishing rate success if used appropriately, but could also raise suspicions in users and decrease compliance if used incorrectly. Specifically, the source of the email, which corresponds to the authority principle, displayed an increase over time in educational institutes ($r_s(850) = .21$, $p < .001$), but a decrease in financial institutions ($r_s(850) = -.18$, $p < .001$). Similarly, the liking/similarity principle revealed an increase over time of logos present in emails ($r_s(850) = .18$, $p < .001$) and decrease in service details, such as payment information ($r_s(850) = -.16$, $p < .001$).

The results from this study offer a different perspective regarding phishing. Previous research has focused on the user aspect; however, few studies have examined the phisher perspective and the social psychological techniques they are implementing. Additionally, they have yet to look at the success of the social psychology techniques. Results from this study can be used to help to predict future trends and inform training programs, as well as machine learning programs used to identify phishing messages.

HotSOS'16, April 19-21, 2016, Pittsburgh, PA, USA.
ACM 978-1-4503-4277-3/16/04.
http://dx.doi.org/10.1145/2898375.2898382

CCS Concepts

• Security and privacy → Human and societal aspects of security and privacy → Social aspects of security and privacy

Keywords

Phishing, Persuasion, Social Engineering, Email, Security

REFERENCES

[1] Akbar, N (2014). *Analysing Persuasion Principles in Phishing Emails.* Unpublished Master's Thesis. University of Twente. Enschede, Netherlands.

[2] Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. New York: Collins.

[3] Ferreira, A., & Lenzini, G. (2015, July). An analysis of social engineering principles in effective phishing. In *Socio-Technical Aspects in Security and Trust (STAST), 2015 Workshop on* (pp. 9-16). IEEE.

[4] Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., & Mayhorn, C. B. (2014). One Phish, Two Phish, How to Avoid the Internet Phish Analysis of Training Strategies to Detect Phishing Emails. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 58, No. 1, pp. 1466-1470). SAGE Publications