Student: Kurt Williams
Instructor: Diwakar Yalpi
Course: CYSE 201S (19044)
Date: 9/26/2024

Article Review 1: “The Health Belief Model and Phishing: Determinants of Preventative Security Behaviors” by Jie Du, Andrew Kalafut, Gregory Schymik

From Journal of Cybersecurity, Volume 10, Issue 1, 2024, tyae012,
https://doi.org/10.1093/cybsec/tyae012

Introduction

This scholarly article studies the relationship between the health belief model (HBM) and the cyber-attack known as “phishing” in the students, faculty, and staff of a midwestern public university. The authors of this study used HBM as the basis for their theory, and they also used the eight constructs of HBM to test their hypothesis: “email security behavior, perceived barriers to practice, self-efficacy, cues to action, prior security experience, perceived vulnerability, perceived benefits, and perceived severity” to inform how these principles effected how their respondents used cyber security practices to protect themselves.

How the topic relates to the principles of social sciences

As the study notes, cyber crime through e-mail is not a new phenomenon, but there is limited research in using social psychology theories such as HBM as it relates to subjects’ actions and behaviors related to e-mail security. The researchers noted that prior HBM research in cybersecurity has focused on studying only one group at a time, such IT professionals or students. However, this study attempts to study different groups (students, faculty, staff) at the same time to compare and contrast how these different sub-groups are affected by HBM concepts and phishing attacks.

The study's research questions or hypotheses

The authors undertook this study to gain an understanding of the different factors that influenced the preventative behaviors of students, faculty, and staff related to phishing attacks through e-mail. According to the authors, “The HBM was chosen as the theoretical basis for this investigation because it is an expectancy-based theory defined to explore the drivers of preventative behavior.” Per the article, “The HBM relies on the notion that if a person believes that an action will reduce the risk of something occurring, they will most likely take that action”, and the researchers teste this theory in their study to see if HBM constructs also informed how respondents approached their e-mail security. Furthermore, the researchers “posit that, if a person feels they may be vulnerable to a phishing attack, they will likely be on the lookout for it and take action to avoid being victimized.”

Types of research methods used

The researchers used a single, large-scale electronic survey of student, faculty, and staff regarding their e-mail security practices and behaviors, which allowed for a much broader sample of respondents. The survey used eight demographic variables, 32 email security questions, and the survey was intended to be completed in less than 10 minutes. The respondents included randomly selected students, faculty, and staff at one midwestern university in the United States. The survey was sent to the respondents via email in November 2019.

Student: Kurt Williams
Instructor: Diwakar Yalpi
Course: CYSE 201S (19044)
Date: 9/26/2024

Types of data and analysis done

The survey focused on using the eight constructs, one dependent on variable and seven independent variables. Approximately 1700 emails were randomly selected, and the researchers assumed a response rate of ~10%. The study received 489 responses, but 61 responses with missing answers, and 10 decline responses were not used. This left 418 responses that were used in the study. The different subgroup sizes broke out into 101 students and 317 faculty/staff. There was also a 61/39 female to male ratio with students and 55/45 female to male ratio for the faculty/staff. The researchers used two steps in their analysis of the data collected. First they used an exploratory factor analysis (EFA) to remove latent variables. This EFA was also used to validate the researchers' model constructs. Next, the researchers conducted a multiple regression analysis to calculate the scores for each factor using the Statistical Package for the Social Sciences (SPSS) software program.

Conclusion

In their abstract, the authors claim "The findings of this study may help shed light on how universities can better prepare students, faculty, and staff to handle this critical information security concern. Given the makeup of the subject population, some findings may be applicable to businesses beyond academic institutions." The authors noted that cybersecurity, especially through email, is one of the top concerns for university administrators. However, three key findings from the study included: 1) "Perceived severity was not found to be a significant determinant of email security behavior in any of the analyses (whole sample, faculty/staff, and student subgroups)." 2) "Similarly, cues to action was not found to be a significant determinant in any of the analyses." 3) "Self-efficacy was the only factor found to be a significant determinant in all three analyses." Overall, this study shows that there is still a lot of work needed to be done in order to understand how the HBM constructs can inform email security behaviors in the university environment.