

Article Review #2: Analysis of Behavioral Reactions to Phishing Scams

Student Name: Zachariah McDonough

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/04/2026

Introduction

Phishing has been one of the most constant and persistent threats to cybersecurity due to its exploitation of human nature instead of mere vulnerabilities in technology. Typical awareness programs will usually fail as a result of ignoring these underlying psychological factors. Wherefore this article by Dr. Gwenhure deals with this gap by utilizing the Health Belief Model (HBM) to look at university students' responses to email phishing attacks.

Connection to Social Science Principles

The article has a significant connection to social sciences principles from its utilization of psychology and behavioral science. This is because the article specifically uses the Health Belief Model, which is meant to explicate how peoples' views of threat and efficacy affect prophylactic measures. Although originally the model was developed for particularly health behaviors like vaccination or disease prevention, but here it has been extended to cybersecurity. Important HBM concepts are perceived susceptibility (i.e., risk of harm), perceived severity (i.e., seriousness of consequences), perceived benefits/importance, perceived barriers, self-efficacy (i.e., confidence in one's ability), and cues to action (i.e., triggers that prompt behavior).

Furthermore, the article additionally relates to decision-making theory and cognitive psychology by displaying how people's beliefs and perceptions can shape their behavior under uncertainty. Moreover, the article addresses the sociological aspects of technology use among what it calls "digital natives" (viz. university students) and the role that social cues or awareness programs have in influencing collective security practices (Gwenhure, 2025). As stated, these principles demonstrate that cybersecurity is not a mere technical issue but a human and social one.

Research Question and Hypothesis

The research question of this article would be what cognitive and emotion factors (that are taken from the HBM) affect university students' security behaviors in response to email phishing attacks. Furthermore, the article treats of six directional hypotheses. The first is that the perceived susceptibility positively correlates with security behavior, which was rejected. Secondly, that perceived severity positively correlates with security behavior, this was supported. Thirdly, that perceived importance positively correlates with security behavior, and this was strongly supported by the evidence. Fourthly, that perceived barriers negatively correlate with security behavior, which was rejected. Fifthly, that self-efficacy is something that positively correlates with security behavior, that was supported. And lastly, that cues to action positively correlate with security behavior, likewise being supported by the evidence.

There were six independent variables, to wit, the six HBM constructs of susceptibility, severity, importance, barriers, self-efficacy, and cues to action. The dependent variable was just their security behavior, such as self reported actions like checking links, avoiding any suspicious emails, or them verifying senders. Moreover, Dr. Gwenthure demonstrates his full understanding by linking the hypotheses directly to HBM theory and then discussing why some of the constructs (like susceptibility) may not truly predict behavior in this context as a result of certain factors like optimism bias or rarely using their email.

Research Methodology and Data Analysis

This article is a quantitative and cross-sectional survey study which utilizes a positivist approach. Specifically, the data came from a convenience sample of 569 university students from Universitas Atma Jaya Yogyakarta in Indonesia. Though the final N was 535 after data cleaning. The instrument that was used was the Student Cybersecurity Awareness Survey, which is a closed ended questionnaire designed with demographic questions and also Likert scale items (1-5), that was adapted from literature before for each of the HBM constructs. Further, it was first pilot tested then translated into Bahasa Indonesia, finally being distributed via printed QR codes that linked to a google form.

As for data analysis, Dr. Gwenhure states he used SPSS 27 for cleaning, reliability (specifically Cronback's alpha > 0.7), normality, and multicollinearity checks (Gwenhure, 2025). Additionally, he used AMOS 23 for Confirmatory Factor Analysis (CFA) to ascertain the measurement model was valid and did Covariance-Based Structural Equation Modeling to test his structural model and hypotheses. Moreover, the model fit indices were acceptable (his RMSEA was 0.060, CFI was 0.903), and the model was able to explain the 64.5% of variance in the dependent variable.

Connections to the Concerns of Marginalized Groups

University students can represent a group that is considered digitally vulnerable, especially those who are not majoring in IT as well as those from lower socioeconomic backgrounds who due to their upbringing did not have much interaction with technology. As can be observed from the sample, about 50% of students had no cybersecurity awareness program, and only 23.2% had been confirmed phishing victims. Therefore the study shows important

concerns like the digital literacy gaps among students, in addition to optimism bias, and unequal access to efficacious training.

If cybersecurity interventions were tailored toward emphasizing the gravity and importance of phishing, that would provide a particular benefit to those marginalized subgroups within the student populations as mentioned previously. Namely, those in non-technical fields, poor upbringings with lack of interaction with technology, or with otherwise lower exposure to awareness campaigns. Necessarily these are who are most likely to fall victim to phishing scams which lead to identity theft or financial loss. Thus if cybersecurity had more psychologically informed programs instead of a one size fits all approach the programs would be more effective and equitable.

Conclusion

Overall, Dr. Gwenhure's article makes two pivotal societal contributions. Firstly, it advances behavior cybersecurity by successfully adapting the HBM to phishing prevention, and by explaining much of the variance in student security behavior. Secondly, it offers practical guidance for designing a more efficacious and targeted awareness program that specifically focuses on building perceived severity, the personal importance of security, self-efficacy, and timely cues to action; which ultimately improve the individual and thus institutional resilience to phishing.

Reference

Anderson Kevin Gwenthure, University students' security behavior against email phishing attacks: insights from the health belief model, Journal of Cybersecurity, Volume 11, Issue 1, 2025, tyaf034, <https://academic.oup.com/cybersecurity/article/11/1/tyaf034/8313771>