Article Review #2: The Health Belief Model and Phishing: Determinants of Preventative Security Behaviors

Student Name: Mario Martinez

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/16/2025

BLUF: The article explores the cyber hygiene of students and faculty at a university, specifically investigating their susceptibility to email based attacks. The article's finding is that the user's perception of their vulnerability and the severity of them are key indicators of the strength of their security practices using email.

Introduction

The article *The Health Belief Model and Phishing: Determinants of Preventative Security Behaviors*, is a cybersecurity research article focusing on the level of cyber hygiene surrounding email usage by university students and professors at an unnamed midwestern university. The article revolves around what it calls the 'Health Belief Model' as a theoretical measurement device to determine the cyber hygiene of a person based on key factors revolving around their personal perception of the strengths and weaknesses of their security posture. It measures the categories of: email security behavior, perceived barriers to practice, self-efficacy, cues to action, prior security experience, perceived vulnerability, perceived benefits, and perceived severity. Barriers to practice, self-efficacy, vulnerability, benefits, and prior experience. The study collected data through the use of surveys distributed to students and faculty.

Connection to Social Science Principles

This article connects to the social science principles of relativism, determinism, and empiricism. The article is relevant to relativism because it attempts to draw a relationship between cyber vulnerability in email and personal perception of vulnerability and personal security. Similarly, it is strongly linked to determinism because it is making the case that personal perception and behavior is a direct predictor of the level of vulnerability. Finally, because the study utilized collected study data as the basis to analyze under the 'Health Belief Model' it demonstrates empiricism.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

The article's research question is: *How well do portions of the Health Belief Model predict email cyber hygiene?* The proposed hypothesis was that higher perception of vulnerability would predict better cyber hygiene (and vice-versa). The independent variables were the users perception of vulnerability to and severity of an email cyber attack against them. The dependent variable was the security best practices and methods reported by users to avoid becoming victimized.

Types of Research Methods used

The data collected in the study was collected via a survey distributed through multiple formats on one university campus to faculty and students in an Introduction to Computing class, and participation was voluntary. According to the article, 153 usable responses were returned. The data collected was quantitative, as the level of belief in the users own practices is what the survey was seeking to record and measure.

Types of Data Analysis used

The article makes use of the Health Belief Model (HBM) as a tool to measure and analyze the data that was collected. The research team performed an Exploratory Factor Analysis (EFA) using the 8 categories of the HBM. The results of the EFA were then used to conduct a statistical regression analysis to determine the likelihood of a certain perception being a key predictor of the strength of user best practices and cyber countermeasures.

Connections to other Course Concepts

In class, we talked about Cyber Victimization and factors that can increase your risk for it, and this study seems to align with that discussion well. For example, the study seems to really explore the idea of optimism bias; i.e. people don't think that bad things will happen to them. In

this study those who perceived themselves as at risk or vulnerable, turned out to have better habits. Meanwhile those that arguably had optimism bias, who did not seem particularly worried, trended toward being more vulnerable. While it was not measured directly in the study, it would probably be fair to say those individuals who did not perceive themselves as vulnerable are generally high in agreeableness, and thus they are more vulnerable.

Connections to the Concerns or contributions of Marginalized Groups

While not directly referenced in the study, I would be interested in cross-referencing this dataset with data on the respondents socio-economic background and educational background. I would contend that those of lower socio-economic status and are less likely to have regular access to or need for email are likely to have had lower levels of perceived vulnerability and thus higher levels of actual vulnerability. Groups like this would need to receive additional education and training on basic cyber hygiene to give them a realistic understanding of their vulnerabilities. Additionally, groups from non-western cultures may have lower levels of social trust due to their cultural backgrounds, and thus may not be totally forthcoming with the information this study is using to evaluate the user. So I would contend those groups may need a different evaluation tool to properly be gauged.

Overall societal contributions of the study

This article is a fairly useful and practical contribution to cybersecurity and social science, because it draws a direct measurable link between perception of vulnerability to cybercrime and actual vulnerability to cybercrime. The results of the study would seem to imply that worrying about your cyber hygiene is a positive indicator of good cyber hygiene, and so I would contend that the way to get net-positive results in cybersecurity it get people in a state where they are concerned and worried about how secure their cyberspace presence is at any time.

Basically, if you can get more people worried about it, they will do something about it, and you will create a net-positive cybersecurity posture. Additionally, as the study itself says it was able to capture a cross section of different student and faculty groups by surveying a university, so another benefit is that this data can probably be readily extrapolated to and transposed onto other institutions to gauge their cyber hygiene and potential for cyber victimization.

Reference

Article Link: Du, J., Kalafut, A., & Schymik, G. (2024). *The health belief model and phishing: Determinants of preventative security behaviors*. *Journal of Cybersecurity, 10*(1), tyae012. https://doi.org/10.1093/cybsec/tyae012