Article Review#2: **University students' security behavior against email phishing attacks: insights from the health belief model**

Student Name: Jared Peel

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Yalpi

Date: 4/15/2026

BLUF

In this article, student response to phishing threats is examined in university environments and why the failure of change to behavior takes place regardless of cybersecurity awareness efforts, highlighting human behavior rather than the technological aspect.

Social Science Principles Connections

This article incorporates several social science principles with the focus being human behavior. The Health Belief Model, which is a social science theory that explains choice for people to choose or disregard behaviors that protect them. The point being, cybersecurity is nowhere near just technical, and the dependence on human perception of risks, consequences, and benefits is just as if not more important than the technical aspect. “Introduced in 1952, the Health Belief Model is a psychological framework utilized to understand and forecast health-related behaviors [51] and later applied to understand why individuals either implement or neglect preventive practices [52]. The HBM suggests that a person’s perceptions about a health condition influence their response to it [53,54]” (Kevin 1).

Research Question /Hypothesis/ Independent Variable/Dependent Variable

The main research questions that the article address are; Why does behavior fail to change despite the awareness programs that exist? What are the factors that affect students' capabilities to identify and reply to phishing emails? Kevin proposes several hypotheses that are focused on the Health Belief Model such as "students who take phishing serious are more secure around it." As well as "What action is taken depending on the benefits that are presented, vs the negatives." Independent variables include the perceptions of susceptibility, severity, negatives, benefits, and self-efficacy. Dependent variable is student behavior, and how they respond to phishing emails.

Types of Research Methods

The main research method used is quantitative data using surveys and other types of questioning. As well as the theory approach using the Health Belief Model and comparing data between the two methods to come to consistent conclusions.

Types of Data Analysis Used

The examination between behavior and perceptions are highlighted analyzing how cyber actions are influenced by psychological factors. As well as statistical methods to gather data to support the examinations.

Connections to other Course Concepts

Connecting module eight presentation to this article, the concept of sociology relates to this article perfectly. Sociology is the study of social life, changes, and consequences of human behavior, as well as the causes of that said behavior. This whole article could be an extended topic of sociology, obviously focusing on phishing attacks.

Group Concerns

Marginalized groups that are not accessible to cybersecurity education are more vulnerable to phishing and will not have the correct behavior and preceptions to deal with it and react correctly. Digital literacy and training are some unfortunate things that lesser individuals will miss out on. Awareness programs do not acknowledge and consider the differences that exist. Unequal exposure is inevitable.

Contributions to society/Conclusion

This article promotes the idea that behavioral change will not occur with awareness by itself. Cybersecurity strategies that contain behavioral strategies are needed, and organizations gain assistance in security policies, training, and programs from this. Phishing attack protection is increased with this article's teachings, and a more human approach to cybersecurity is

emphasized. Cybersecurity is nowhere near just a technical issue, and the social aspect is just as important.

Reference

Gwenhure, Anderson Kevin. “University Students’ Security Behavior against Email Phishing Attacks: Insights from the Health Belief Model | Journal of Cybersecurity | Oxford Academic.” *Oxford Academic*, 4 Nov. 2025, academic.oup.com/cybersecurity/article/11/1/tyaf034/8313771.