

**Article Review #2: University Students' Security Behavior Against Email Phishing Attacks:
Insights from the Health Belief Model**

Student Name: Tenny Boone

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/16/2026

Introduction/BLUF

This article examines how university students respond to email phishing attacks using the Health Belief Model. The study focuses on understanding how psychological factors like perceived severity, self-efficacy, and cues to action aid in influencing cybersecurity behaviors. Overall, the findings suggest that human behavior and not just technology plays a huge role in preventing the possibility of cyberattacks. This highlights the growing importance of behavioral cybersecurity and shows that improving user awareness and their decision making process is just as important as implementing technical defenses and security measures.

Relation/Connection to Social Science Principles

The article strongly showcases the core principles of social science research. First, the principle of empiricism is demonstrated through the collection of real data from 569 students at the university using surveys. The study relies on measurable evidence and not assumptions. Second, objectivity is maintained through the use of statistical tools such as Structural Equation Modeling which allows the researchers to analyze relationships between variables without involving their personal bias. Third, skepticism is evident in the testing of the 6 hypotheses because not all expected relationships were supported and this shows that the researchers critically evaluated the assumptions that they made. Fourth, the principle of parsimony is reflected in the use of the Health Belief Model because it simplifies many complex human behaviors into a structured variety of variables. Fifth, determinism can be found in the article because the study assumes that behavior is influenced by identifiable factors such as beliefs and perceptions. Sixth, ethical neutrality is established through the unbiased reporting and the protection of each participant's confidentiality. Finally, relativism is shown by recognizing that

cybersecurity behavior can vary across many different populations meaning that the findings may be different in other groups outside of university students.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

The research questions in the article focus on identifying which psychological factors help influence students' behavior when it comes to phishing attacks and how effective the Health Belief Model is when it comes to predicting cybersecurity behavior. The study proposes 6 specific hypotheses: Perceived susceptibility will demonstrate a statistically significant positive correlation with security behavior, perceived severity will demonstrate a statistically significant positive correlation with security behavior, perceived importance will demonstrate a statistically significant positive correlation with security behavior, perceived barriers will demonstrate a statistically significant negative correlation with security behavior, self-efficacy will demonstrate a statistically significant positive correlation with security behavior, and cues to action will demonstrate a statistically significant positive correlation with security behavior. These hypotheses imply that perceived severity, perceived importance, self-efficacy, and cues to action positively influence security behaviors while perceived barriers negatively affect it. The independent variables in the study include perceived susceptibility, perceived severity, perceived importance, perceived barriers, self-efficacy, and cues to action. The dependent variable is the students' security behaviors, specifically how they respond to phishing threats and the ways that they protect themselves from cyber risks.

Types of Research Methods Used

The study uses a quantitative research method with a positivist approach. Data was collected through a structured questionnaire distributed to students attending Atma Jaya Yogyakarta University using convenience sampling. This method allowed the researchers to

gather a large amount of data efficiently and test their hypotheses using statistical analysis. The focus on measurable variables and hypothesis testing aligns with traditional scientific research methods commonly used in social sciences.

Types of Data Analysis Used

For data analysis, the researchers performed several statistical methods to ensure that their findings were reliable. The methods included descriptive statistics to summarize participant demographics and behavior patterns, reliability testing using Cronbach's alpha to ensure that the data was consistent, Confirmatory Factor Analysis to validate the measurement model, and Structural Equation Modeling to help analyze the relationships found between the variables. These methods allowed the researchers to determine which psychological factors had the most significant impact on cybersecurity behaviors.

Connections to other Course Concepts

The article connects to multiple concepts discussed throughout the course, particularly the ones related to sociology, human-centered cybersecurity, and social forces. First, the study strongly aligns with the concept of human-centered cybersecurity because this concept emphasizes that human behavior is crucial to security outcomes. The study done by these researchers demonstrates that students' beliefs, perceptions, and decision-making directly influence whether they fall for these attacks. The article also connects to sociological perspectives on behavior, as discussed in Module 8, where sociology examines how outside influences shape human actions. The students' responses to phishing can be understood through social forces such as education and peer influence which shape cybersecurity awareness and behavior. The findings also relate to the topic of cybersecurity culture found in Module 9, where beliefs, normalized things, and values influence how individuals act online. The study shows that

students who perceive cybersecurity as important are more likely to use safer practices. This reinforces the role of cultural norms in cybersecurity behavior. Finally, the article connects to social cybersecurity concepts because they focus on understanding and predicting human behavior when it comes to cyber environments. The research aligns with the goal of analyzing how individuals respond to cyber threats and how those responses can be improved to reduce risks. Overall, the article goes to show how cybersecurity is deeply connected with social science concepts like human behavior, social structures, and cultural influences.

Connections to the Concerns or contributions of Marginalized Groups

The topic of this article also relates to the challenges and concerns of more vulnerable groups. While university students are not always considered a vulnerable population, they can be seen as vulnerable due to limited cybersecurity training given to adolescents, their lack of experience, and being too confident in their digital skills. Students from less resourced backgrounds may have even less access to cybersecurity information which increases their risk of falling for possible phishing attacks. The consequences of these attacks are financial loss and identity theft and these consequences can heavily shift individuals' lives that have fewer resources. By focusing on awareness and behavioral change, the study contributes to improving cybersecurity protection for the more vulnerable groups.

Overall societal contributions of the study/Conclusion

In conclusion, this study makes important contributions to society by emphasizing the role of human behavior in cybersecurity. It demonstrates that technical solutions alone are not enough to prevent cyber threats from happening and that understanding psychological factors is a key factor for improving security outcomes. The findings can help organizations develop more effective cybersecurity awareness programs that target user behavior rather than only relying on

technology. Essentially, the study supports the integration of social science theories into cybersecurity research, hoping for a safer digital environment.

Reference

Gwenhure, A. K. (2025). University Students' security behavior against email phishing attacks: Insights from the health belief model. *Journal of Cybersecurity*, 11(1).
<https://doi.org/10.1093/cybsec/tyaf034>