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

Student Name: Adrian Valencia

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Yalpi

Date: November 11, 2025

## Introduction/BLUF

In 2025, a study was conducted by Anderson Kevin Gwenhure investigating the university student victims to phishing email attacks through the psychology Health Belief Model (HBM). From a sample survey of 569 students, researchers concluded that perceived severity, perceived importance, self-efficacy, and cues to action were the motivating factors that predicted the student's security behavior, leaving out perceived susceptibility and barriers. Ultimately, a person's psychological state and their normal behavioral facts are what determines their cybersecurity awareness.

## Relation/Connection to Social Science Principles

The study connects to the principles of social science through different parts of the study. For example, empiricism can be seen through measurable data and testing that is used to understand the students cybersecurity behaviors. Determinism is shown in the results where relationships of psychological beliefs is the determining and causing factors of how a student reacts to the phishing attempts. A third principal parsimony is brought in the study with the use of the Health Belief Model (HBM) that allows for an easier understanding of behavior in relation to phishing attacks. The researchers show objectivity through the data by the methods used to ensure that there is no bias between the data and how it was gathered. The study involves skepticism all around, from putting things through tests by questions of claims from the students. Additionally, with regards to the study, research designed the survey to protect the anonymity of the participants by avoiding personal bias. The last principle relativism can be seen with the behavior in cybersecurity where the influence is similar but varies between a person's experiences. In essence, the use of these principles allows us to further our research and knowledge of cybersecurity in correlation to psychology, showing that human behavior shapes the future of technology.

## Research Question/ Hypothesis/Independent Variable/Dependent Variable

The main research question that the study works to investigate is "Which psychological and behavioral factors influence university students' cybersecurity behavior toward email phishing attacks?" (Gwenhure, 2025). Following the research question, six hypotheses were created with regards to security behavior and a person's psychological state. However, the main hypothesis were that perceived severity, perceived importances, cues to action, and self-efficacy will be a positive effect on the student's security behavior. The second main hypothesis was that perceived susceptibility and barriers will have a negative effect on the students' relationships on cybersecurity behavior. To conduct the study the independent variable measured was susceptibility, severity, importance, barriers, cues to action, and self-efficacy. The dependent variable measured was how the students reacted against phishing attempts.

## Research Methods Used

In the study, the researcher used a quantitative method with a focus on the behavior of the participants with regards to the social sciences. This was done through a survey called the Student Cybersecurity Awareness Survey which was created and inspired through the Health Belief Model. The data was then measured through a Likert-Scale survey which evaluated a person's characteristics through a small convenience sampling from the university.

## Data Analysis Used

The data in the study was analyzed through the Confirmatory Facto Analysis in addition to Covariance-Based Structural Equation Modeling. Through the analysis using these two tools, a summary of variable relationships and the validity of the measurement was ensured. The covariance model allowed researchers to conclude that psychological variables explained the reason behind the actions of the students cybersecurity behavior. The supporting factors of the statistic results were the self-efficacy, perceived importance, cues to action, and perceived severity which were the factors in the hypothesis. Ultimately, the data and findings prove that character behavior and consequences are what motivate security actions.

## Connection to other Course Concepts

In relation to the class concepts, the study hits many topics that was discussed within the class. For example, the study connects to the interdisciplinary nature of cybersecurity, and the psychology, sociology, and criminology reflect on human engagement with technology and how it is used. The HBM shows the social learning theory awareness of attacks and the repetition of recognizing shape a more secure lifestyle. Furthermore, the idea of a human firewall relates to the study because of how awareness shapes the protection on all levels. More importantly, a person always is the first line of defense. To relate to the course concepts, cybersecurity is more broad than technology but is a field of social science itself.

## Connections to the Concerns or Contributions of Marginalized Groups

The study did not have contribution with marginalized groups specifically but touches on digital equity and inclusion. More specifically, the students all have different backgrounds like low income or different majors. This means that each person reacts and may react differently from others when it comes to cybersecurity exposure. This shows and explains the results of a reduction in self-efficacy within the study. Adding on, the different background reflects on how socioeconomic disparities in the technical world and of the students awareness in cybersecurity. This is a topic that must be addressed through training and other awareness methods to help improve cybersecurity protection around the world. The study adds to how social inequality can lead to certain people vulnerable to attacks.

## Overall Societal Contributions of the Study/Conclusion

In essence, the study and research conducted by Gwenhure contributes to society through behavioral dimensions in regards of cybersecurity. The research demonstrates psychological

beliefs and perceptions influence a person's vulnerability to phishing attacks. The results indicated that people in society need to encourage and support more educational guidance that alerts people of attacks and to help with behavioral awareness to highlight the risks in the real world. The social science theories allow for further development within the cybersecurity industry as shown in the study. It opens perspectives of understanding about human behavior that can be used to protect our online risks. In conclusion, the research helps educate about cybersecurity and the social sciences through our security and the culture awareness of the people.

## Reference

Gwenhure, A. (2025, November 4). *University Students' security behavior against email phishing attacks: Insights from the health belief model | journal of cybersecurity | oxford academic*. Journal Of Cybersecurity. https://academic.oup.com/cybersecurity/article/11/1/tyaf034/8313771