Tammy Rizo

October 11, 2026

Understanding Human Behavior in Phishing Prevention

Introduction

Approaching cybersecurity through an interdisciplinary lens, it is understood that protection comes from understanding human factors and how they influence our choices. In the article "The Health Belief Model and Phishing: Determinants of Preventative Security Behaviors," Du et al. (2024) examine how a person's perceptions, beliefs, and experiences can influence their email security behaviors. A theory called the Health Belief Model (HBM) was used to explain why some people take preventive action, and others do not. This helps them to understand how people respond to phishing threats.

Social Science Principles

Several principles of social science, such as empiricism, objectivity, and ethical research, are included in this research. Empiricism involves collecting evidence through observation and research. The researchers collected survey responses to examine how people's beliefs influence their cybersecurity behaviors. You can not just rely on personal opinions. Principles such as objectivity and ethical research helped researchers develop reliable findings while considering the rights of participants. Objectivity is important because researchers must evaluate evidence. Du et al. (2024) used statistical analysis to test their hypotheses and identify relationships between different factors. Ethical research is another important principle used here because the researchers received approval from their university's Institutional Review Board before conducting the survey.

Research Questions, Hypotheses, Research Methods, and Data Analysis

The main focus of this study was to understand the factors that influence people to practice preventive email security behaviors. They hypothesized that people who believed they were vulnerable to phishing attacks and felt they could recognize threats would be more likely to practice safe email behaviors. They also hypothesized that students and university employees would differ in which factor would influence their decisions (Du et al., 2024). The researchers examined whether factors such as perceived vulnerability, perceived severity, perceived benefits, perceived barriers, self-efficacy, and prior experiences influenced how people made their security decisions.

An online survey was conducted at a public university. Quantitative research methods were used to collect and analyze the data (Du et al., 2024). They received 489 responses. The surveys included 101 students and 317 faculty and staff members. Exploratory factor analysis was used to examine how the survey questions measured different factors. They also used multiple regression analysis to determine which factors were significantly associated with reported email security behaviors. They discovered that self-efficacy was the only factor significantly associated with email security behavior in all three analyses. This shows us that people's confidence in their ability to identify and avoid phishing attacks was an important factor for both students and employees. The research showed that prior experience was significant for students. Perceived benefits were significant for employees. The findings show us that different groups need different approaches to cybersecurity training (Du et al., 2024).

Connections to Course Concepts

This study applies several concepts that we discussed in class. Concepts such as social engineering, social influences, cybersecurity culture, cognitive bias, and cyber victimization. Phishing is a form of social engineering that manipulates people into revealing sensitive

information or taking unsafe actions. Social influences can affect how individuals learn about cybersecurity and develop security habits. Cybersecurity culture plays a big part in our influences. Organizations and universities need to encourage employees and students to practice safe cyber behaviors. Cyber victimization is relevant to the study because phishing attacks can lead to identity theft. Financial losses and unauthorized access to personal information could also result from these attacks. A victim should never be shamed for falling for an attack in situations like this. These concepts teach us how human behavior and social environments influence cybersecurity.

Marginalized Groups

One concern for marginalized groups in this study is unequal access to cybersecurity education and training. Individuals with limited educational opportunities or digital literacy may have a hard time recognizing phishing attacks. Another concern is economic inequality. People with limited financial resources may have fewer opportunities to access cybersecurity training or reliable technology. These challenges could increase their vulnerability to cybercrime. The researchers did not specifically examine marginalized populations, but it is understood that cybersecurity education should consider the different experiences, abilities, and resources of individuals.

Conclusion

The study by Du et al. (2024) demonstrates the importance of understanding human behavior in cybersecurity. This research can help universities and organizations develop more effective cybersecurity awareness and training programs. Another contribution is identifying differences between students and employees that may help organizations develop training appropriately for different groups. The research also shows how social science theories and

quantitative methods can be used to understand cybersecurity problems. Overall, the study reinforces that protecting information requires more than technology. It also requires understanding people's beliefs, experiences, and decisions.

References

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