Article Review #2: Cybersecurity, Social Behavior, and Online Victimization

Name: Jacob E. Moore

Date: April 14, 2026

Introduction

The article selected for this review is *"Cybercrime Victimization and Online Behavior"* from the International Journal of Cybercriminology. This study focuses on how individuals' online behaviors can increase or decrease their risk of becoming victims of cybercrime. As

technology continues to grow, understanding the human side of cybersecurity becomes just as important as the technical side. This article highlights how user behavior, awareness, and decision-making all play a role in cybersecurity risks.

Connection to Social Science Principles

This topic directly relates to social science principles, especially in the areas of psychology and sociology. One key concept is **routine activity theory**, which suggests that crime occurs when a motivated offender, a suitable target, and lack of protection come together. In the context of cybersecurity, users who engage in risky online behavior (such as clicking unknown links or sharing personal information) can become easy targets. Another important concept is **human** behavior and decision-making. The article shows how people often underestimate cyber risks or prioritize convenience over security, which increases their vulnerability.

Research Questions, Hypotheses, and Variables

The main research question of the study is: How do online behaviors influence the likelihood of becoming a victim of cybercrime? The study hypothesizes that individuals who engage in higher-risk online activities are more likely to experience cybercrime victimization.

- Independent Variable: Online behavior (such as internet usage patterns, social media activity, and risk-taking behavior)

- Dependent Variable: Cybercrime victimization (whether an individual has been a victim of cybercrime)

Research Methods

The researchers used a quantitative research method, collecting data through surveys. Participants were asked about their online habits, awareness of cybersecurity, and any experiences with cybercrime. This method allows researchers to identify patterns and relationships between behavior and victimization across a large group of people.

Data and Analysis

The data collected included self-reported information about internet usage, online habits, and past experiences with cybercrime. The researchers used statistical analysis to determine whether there was a relationship between risky behavior and victimization. The results showed a clear connection of individuals who engaged in more risky online behaviors were more likely to become victims. This supports the hypothesis and reinforces the importance of user awareness in cybersecurity.

Connection to Course Concepts

This article connects strongly to concepts discussed in class, especially the idea that cybersecurity is not just technical but also behavioral. Topics such as risk management, threat awareness, and human factors in cybersecurity are clearly reflected in the study. It also aligns with discussions about how attackers often target human weaknesses instead of technical systems, which is a key concept in cybersecurity education.

Impact on Marginalized Groups

The study also relates to challenges faced by marginalized groups. Individuals with limited access to cybersecurity education or resources may be more vulnerable to cybercrime. This includes lower-income populations, older adults, and individuals with less technical experience. These groups may not have the same level of awareness or protection, making them easier targets for scams, identity theft, and online fraud. This highlights the importance of making cybersecurity education more accessible and inclusive.

Contribution to Society

This study contributes to society by showing that improving cybersecurity is not just about better technology, but also about improving user behavior and awareness. It emphasizes the need for education, training, and better communication about online risks. By understanding how

behavior affects cybersecurity, organizations and individuals can take steps to reduce risk and protect themselves more effectively.

Conclusion

Overall, this article provides valuable insight into the relationship between online behavior and cybercrime victimization. It reinforces the idea that cybersecurity is a shared responsibility between technology and human behavior. As cyber threats continue to evolve, increasing awareness and promoting safer online habits will play a critical role in reducing cybercrime and protecting individuals.

Reference

Leukfeldt, E. R. (2014). *Cybercrime victimization and online routine activities*. International Journal of Cybercriminology.
https://www.cybercrimejournal.com