Article Review #2: Cybercrime and Online Victimizing

Student Name: Leyah Knox

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Yalpi

Date: 4/14/2026

Introduction/BLUF

The journal I will be using analyzes cybercrime victimization by including some of the social science frameworks, by showing that online exposure, behavior, and environment factors can increase the likelihood of being a victim. The journal also shows cybercrime is not all about technology, but it's also about seeing how human behavior can have patterns, and structural differences. Knowing these frameworks are essential for improving cybersecurity awareness and prevention strategies.

Relation/Connection to Social Science Principles

The journal uses a couple of social science principles, but I am only going to go over the few I feel as though need to be said. It uses relativism because it shows how cybercrime risk can vary depending on a person's behavior, environment, and even social contexts. Some people even have their own ways of defining risky behaviors on the internet and from different users. I've also witnessed a bit of Ethical Neutrality because these researchers don't judge these victims, but they focus on explaining the constant patterns of behavior and risk factors done by offenders or other users. The last one I'll be talking about is Determinism because it suggests that cybercrime victimization is mostly influenced by factors such as routine behavior, lack of protection, and exposure.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

- Research Question: How do online activities influence cybercrime victimization?

- Hypothesis: People who continuously engage in high risk online behaviors tend to become victims of cybercrime.
- Independent Variable: Online routine activities – information sharing/internet exposure
- Dependent Variable: Cybercrime victimization

- This shows the clear relationship between those doing risky online behaviors and increasing the fact people are more likely to be victimized

Types of Research Methods used

I feel like the researchers used quantitative research design, only because it primarily relies on structured surveys to gather data from their participants. Using this method allows them to use measurable comparisons between different outcomes and behaviors of people. Some testing is also used to show the strength of the relationships between variables, which makes the studies reliable.

Types of Data Analysis used

The authors use quantitative data. Some of the methods they used are survey responses, demographic information, descriptive statistics to also summarize participant behavior, and correlation analysis so they can measure the strength of their participants. This helps identify the patterns of how strongly this online behavior predicts victimization.

Connections to other Course Concepts

Identify and elaborate on connections between the study and concepts learned in our course using the PowerPoint presentation from the modules. How does the study reinforce or challenge those concepts?

Connections to the Concerns or contributions of Marginalized Groups

- Cyber Victimization

- Behavior patterns

- Human factors in cybersecurity

This allows the idea that cybersecurity is mostly influenced by its users behavior, and not only with technical devices.

Overall societal contributions of the study/Conclusion

In conclusion, this journal demonstrates that cybercrime is connected to a good bit of social science principles such as relativism, Ethical Neutrality, and determinism. By reading over the routines of behavior online, this journal shows that online victimization is and can be influenced by predictable behavioral patterns. This shows that improving cybersecurity doesn't just involve technological solutions but also rather a strong understanding of the human behavior behind all of this. After doing this research it does give me a more informed mindset of what goes on behind these screens.

Reference

Leukfeldt, E. R., & Yar, M. (Year). *Applying routine activity theory to cybercrime victimization*. *International Journal of Cybercriminology*.

Article Link:

https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123