Jose Gonzalez

09/30/24

Article Review #1: A review of “Integrated Model of Cybercrime Dynamics” and its connection to social science

The article written by Dr. Troy Smith discusses a proposed new model to investigate cybercrime and its causes. While it may not show a true analysis of a specific experiment, it does allow others to experiment with the model and find ways to apply it.

Connection to Social Sciences

One way that this article is connected to social science is that it connects to the principle of determinism. In the article, the author states “The first relationship posits that personality traits, gratification-seeking motives and social norms significantly influence an individual’s online behavior” (Smith, 2024). This quote from the article shows that specific motives and influences let the individual choose what they do online. The second way this article connects to social science is by relativism. For instance, the article shows a figure that shows the structure that is being presented in the article. This diagram shows relativism by showing how each relationship is connected to cybercrime and the people involved. The last way this article relates to social science is by showing skepticism. In the article, the author discusses how theories like routine activities are good starting points but doesn’t give the full picture on cybercrime.

Research Questions and Methods

While there are no direct research questions presented in the article, the main question that is implied from the article is “What kinds of characteristics are present in cybercriminals and victims that cause cybercrime?” For example, in the diagram the author presents shows “motive (gratification)” on the cybercriminal side and “social norms” on the victim side. While there is also no specific research methods mentioned, there are some that researchers can implement to test. For example, “Longitudinal analyses can examine predictive associations over time and establish temporal precedence.” (Smith, 2024). This research method can help researchers to find possible connections to cybercrime and what causes it.

Types of Data and Analysis Done

While the author did not mention any specific data or analysis done, as this paper presents a model of investigation, it can help others to complete experiments in other ways. For instance, a way that researchers can find, and analysis data might be survey data. This type of analysis may help researchers to figure out how certain emotions connect to cybercrime and their victim choice.

Connection to the Course

The article is connected to the course in many ways. Some of the many concepts that come from the class that are integrated into this article are cyber offending, cyber victimization,

victim precipitation, and determinism. For example, “Social norms delineate the boundaries of acceptable conduct online. Descriptive norms normalize risky self-promotion. Deviant norms valorize hacking” (Smith, 2024). This quote shows all four concepts by describing how a victim’s actions can cause themself to encounter cyber victimization.

Connections to Marginalized Groups

Two ways that this paper connects marginalized groups by providing ways that victims can receive support before and after cybercrime. As said in the article “Support plans can address unhealthy motivations, build capabilities for more cautious online conduct, expand social connections offline, and adopt technical precautions” (Smith, 2024). By implementing support plans, it can help to see why some victims are more vulnerable to attacks.

Contributions of this Article

This article and its proposed method can help society by offering a new way to develop new policies and raising awareness of cybercrimes and their risks. For example, as said in the article “Online safety education in schools can increase awareness of victimization risks associated with identity construction, relationships and information disclosure online.” (Smith, 2024). By increasing awareness in companies and businesses, many policy makers can update or create polices that can punish cybercriminals for their crimes.

Conclusion

Overall, this article can help the field of cybersecurity to figuring out why victims are hacked and why cybercriminals commit cybercrimes. With the implementation of this method in many research experiments, they might be able to solve problems that might not have had a solution.

Resource

Smith, T. (2024). Integrated Model of Cybercrime Dynamics: A comprehensive framework for understanding offending and victimization in the Digital Realm. *International Journal of Cybersecurity Intelligence & Cybercrime*, *7*(2). https://doi.org/10.52306/2578-3289.1163

Https link: https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1163&context=ijcic