Myles Damoah
CYSE 201S
Article Review 1
5 October 2025

Cybercrime Prevention through Psychology

Introduction

The article I reviewed “exploring the psychological profile of cybercriminals" is a well detailed 24-page article that discusses the physiological mind of cybercriminals and how they impact victims,institutions, politics, etc just by their illegal actions in the cyberworld. This directly correlates to the social sciences as it dives into the physiological part of cybersecurity proving that cybercrimes aren't just technical. The question of this study was how understanding the physiological behaviors of cybercriminals can be a positive for cybercrime prevention The study challenged that cybercriminals are influenced by their psychological behaviors and understanding those behaviors can enhance offender profiling and prevent an attack before it happens.

Methodology

To answer the hypotheses in question the researchers of this article decided to conduct case studies. To get as much accurate and credible information as possible, “a detailed search strategy was employed. This involved identifying relevant databases and sources, formulating appropriate search terms and keywords, and systematically retrieving and screening studies.” (Thuyen, Ha, & Kim 2025 p.3)

like Pubmed: Which provides data on the physiological impact of cybercrimes. IEEE Xplore: A digital library for research articles and conference proceedings in the fields of electrical engineering,

computer science, and electronics, offering extensive coverage of technological aspects of cyber security. They also used a comprehensive range of keywords to find articles that directly related to their question. Keywords like “cybersecurity crimes”, “Cybercrime”, “Hacking”, and “Malaware” were all put into scholarly search engines, like google scholar, to find more information related to the subject matter.

Data and Analysis

To collect data in this study, researchers came up with a 3 step rigorous process to analyze the validity and reliability of the case study. This three step process includes; “(i) Study Design: The methodological rigor of the studies, including the appropriateness of the study design and the robustness of the data collection and analysis methods. (ii) Sample Size and Representativeness: The adequacy of the sample size and the representativeness of the study population; (iii) Bias and Confounding Factors: Assessment of potential biases and confounding factors that could affect the study's validity.” (Thuyen, Ha, & Kim 2025 p. 4). Using this process, they found various case studies that directly supported their claims.

Relationship to Social Sciences

The article talks about the physiological impact of cybercrime, such as victims always having a sense of vulnerability. This can also be followed up by fear, anxiety, isolation, and many other psychological factors. We can use the Neutralization theory as an example when put with the Sony attack of 2014. State sponsored hackers stole and released sensitive information, employee information, and unreleased films. This event can apply to appeal to higher loyalties. The North Korean backed hackers launched this attack against Sony after they released the

movie “the interview” which painted Kim Jong Un, the leader of North Korea, in a negative light.

This topic challenges the understanding of cyber victimization and sheds light on the fact that there are psychological impacts on people who are victims of cybercrimes. It addresses the gaps in research on combating cybercrime; “several areas remain under-researched. These include the psychological and social impacts of cybercrime on victims, the long-term economic effects on small and medium-sized enterprises (SMEs), and the efficacy of international cyber security cooperation frameworks.” (Thuyen, Ha, & Kim 2025 p. 17).

The article suggests tips for companies when training their employees to become more aware of the potential to be victims of cybercrime. It demands that employers should teach employees the most basic of cyber threats, and set up channels to report suspicious activity to take preventative measures before any real damage is done.

Conclusion

This article helps connect various diverse fields such as, psychology, criminology, sociology, and cybersecurity. This highlights that cybercrime has many contributing factors other than technical skills. Cybercriminals have many factors that feed into their willingness to commit crimes. Which in turn redefines how we profile a potential cybercriminal. Instead of just looking at technically gifted individuals now we start to shift focus on those who do things on impulse, or act in a selfish manner in search of gratification or reward, even those who feel it’s their job to expose vulnerabilities or radicalize a group of people for political power. These are all theories and possibilities that we can now factor in when we look at who a cybercriminal is. This Article has opened the door to the future of cybercrime prevention and how society factors into the equation.

Citation

Thuyen, D., Ha, T. C., & Kim, T. N. (2025). *Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention*. Cybercrime Journal. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/452/133