Jacob Waller 9/28/2025

Cyber Criminals, a Screen as a Face

Introduction

Cyber crime is a growing global threat over the world. Cyber security crimes, also referred to as cyber crimes, encompass a wide range of illegal activities conducted through digital means(International Journal of Cyber Criminology, 2025). This study aims to examine the psychological traits of cyber criminals and how we may prevent future complications. There are two theories that our question or hypothesis relies on. "Routine Activity Theory which was proposed by (Cohen & Felson,1979) ,which suggests that crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of capable guardianship." Our other theory "Deterrence Theory" posits that individuals are less likely to engage in criminal behavior if they perceive the costs (e.g., punishment, loss of freedom) to outweigh the benefits(Williams, 2016).

Psychological Traits of Cyber Criminals: A social science perspective

The psychological traits of cyber criminals also relate to the principle of social sciences. Why would a person continue stealing online versus a person who is not behind a screen "quick to want to stop." Social sciences are the fundamental laws or concepts guiding the systematic study of human society and relationships, including the use of empirical research, ethical considerations, and scientific methodologies to understand social patterns, institutions, and behaviors. Which is what the research in this project was implemented to confront.

Methodology

The strategy used to conduct the research of psychological traits of cyber criminals was "search strategy.""This involved identifying relevant databases and sources, formulating the correct search terms and keywords for retrieving screen studies"(Vol 19, June 2025).

Other Theories

"Criminological theories provide critical insights into the motivations, behaviors, and deterrence mechanisms related to cybercriminals, guiding more effective prevention and mitigation strategies. Several key theories such as routine activity theory, deterrence theory, international cooperation theory, and privacy-security balance theory, help explain cybercrime dynamics and inform policy responses"(Vol 19, January 2025).

Data and Analysis

This review made evident several types of cyber security threats, despite legal frameworks and cyber security measures at both national and international levels. This was revealed in a number of case studies based on their impact and what policies were framed to lower the risk. It was found companies with third party security were more common to find themselves being victimized. "Organizations must adopt a proactive and multi-layered approach to cyber security to mitigate risks and enhance resilience. Enhancing third-party security is crucial, as external vendors often serve as entry points for cyber threats"(Vol 19 issue 1, January 2025).

Psychological Effects on Victims

The psychological consequences of cyber crimes can be very severe. As learned in class, “most cyber victims do not know when they have become one.” Victims of cyberstalking, online harassment, and identity theft often experience chronic stress, anxiety, and depression, as these crimes invade personal spaces and create a persistent sense of vulnerability. All of these things disrupt the basic principles of social science. Unlike usual crimes, a cyber cyber threat can infiltrate someone's life to the point where they are defenseless.

Conclusion

This article explained the research and conducted the experiments necessary to test cyber criminals in a social science perspective. I believe it helps society, letting people know that the world is changing faster than they realize. Criminals nowadays have a keyboard instead of a crowbar. Using past social science theories against them, we may be able to stop crimes before they take place.

Citations.

https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/452/133