Evaluating Socioeconomic Status, Cybercrime, and Victimization

Nicolas R. Stephens

Department of Sociology and Criminal Justice, Old Dominion University

Professor Raelee Passuello

CRJS 215S: Introduction to Criminal Justice

24 September 2025

Evaluating Socioeconomic Status, Cybercrime and Victimization

Today, everything is interconnected; our smartphones can connect to our dishwashers, and our vacuums can connect to servers overseas, making our day-to-day lives vastly more manageable and efficient. This interconnectedness also presents cybercriminals with numerous avenues to attack and steal important information. However, this rise in interconnectivity also provides us with a crucial opportunity to understand the societal implications of cybercrime. We can examine how different socioeconomic backgrounds and demographics are affected by this global phenomenon, and investigate whether those same factors contribute to individuals committing cyber offenses. Understanding these societal implications will enable us to create legislation that targets intervention policies for those at the highest risk and reform societal structures to provide every person with an equal opportunity for a secure digital footprint. More concisely, examining the socioeconomic aspect of cybercrime provides practical insight into which groups are affected and how, as well as how to address the inequality in cyber awareness among marginalized groups.

Regarding the socioeconomic implications of cybercrime, it is important to know the Routine Activities Theory. According to Schram and Tibbetts (2020), "this theoretical framework emphasized the presence of three factors that converge in time and place to create a high likelihood of crime/victimization. These three factors are (1) a motivated offender, (2) suitable targets, and (3) lack of guardianship". Regarding suitable targets, individuals with a poor socioeconomic status or marginalized groups are less likely to have proper training in correct online posture, making them more vulnerable to cyber-attacks compared to those with a higher socioeconomic status who are most likely to have some degree of higher formal education, resulting in a conscious awareness of their cyber posture, and potential implementation of

external precautions to mitigate their risk of attack. Klein (2021) reciprocates the idea that marginalized groups are more exposed in the digital world by stating:

> As more and more people have turned to online work, the opportunities cyber criminals exploit have only increased. Elderly people and those from low income backgrounds who did not receive strong digital education are often the most at risk.

Klein specifically mentions low-income backgrounds because that term encompasses a considerable number of marginalized groups, as mentioned earlier. Concerning specific crimes, Klein states, "Black, Indigenous, and other peoples of color (BIPOC)...were more likely than White respondents to have had their accounts hacked and identities stolen, though they were less likely to be victims of credit card fraud". The assessment that certain cybercrimes are committed in greater numbers against specific groups, while others are not, further exacerbates the fact that socioeconomic status influences an individual's likelihood of becoming a victim of cyber offenders. It also provides information on which crimes are most likely to occur, depending on the individual's socioeconomic status.

Examining the socioeconomic aspects of cybercrime offers insight into where legislation should be targeted to achieve effective change, particularly in areas such as digital literacy and security awareness. There are numerous methods for accomplishing this, such as government programs targeted at low-income areas to spread awareness on basic housekeeping rules regarding internet use. More effectively, legislators could introduce policies for mandatory cybersecurity education in public schools to provide children with basic knowledge of the internet, passwords, data privacy, and other essential topics that are crucial for maintaining a safe online experience.

In summary, by examining the socioeconomic aspects of cybersecurity, not just the crime itself, it is clear that there is a systematic failure to adequately inform individuals of the risks associated with the internet and cybercrime. As a result, it is crucial to implement programs aimed at marginalized groups to inform them of standard safety practices and/or to introduce a mandatory cybersecurity curriculum in public schools, thereby fostering safe cyber practices to protect the next generation from the increasing threat of cybercrime.

References

Klein, D. (2021, July 18). *Report: Minorities and women are more likely victims of Cyber Crime*. OCCRP. https://www.occrp.org/en/news/report-minorities-and-women-are-more-likely-victims-of-cyber-crime

Schram, P. J., & Tibbetts, S. G. (2020). Introduction to Criminology: Why do they do it? (3rd ed.). SAGE Publications, Inc.