https://canvas.odu.edu/courses/188032/assignments/2857687Emmanuel Walker

Diwakar Yalpi

CYSE 201S Cybersecurity and the Social Sciences

9/28/2025

Although cybersecurity is presented as a technology problem, its involvement with human behavior, social structures, and cultural norms makes it related to the ideas of the social sciences. Understanding human interaction and societal outcomes, all of which are key to explaining cybercrime and countermeasures. The role of social science "is essential for equitable cybersecurity solutions because marginalized communities face particular digital threats" (Azariahpugh, 2025), which emphasizes how people use technology in a positive or negative ways that reflect social norms.

Thinking about how technology is evolving throughout the years to not knowing how to use a digital phone, to tracking accurate IP addresses. The use of technology in society is everyday practice and people tend to use it to do positive things or negative things. The research question then becomes what behavioral or sociological characteristics make people more prone to become a victim of cybercrime because people who are less likely to use technology are more likely to be victims of cybercrime because they do not know how the system works. The generation of Gen Z were born into technology, so they are likely to know how to protect themselves while using technology compared to someone who is a baby boomer or Gen X. They would be more likely to be prone to victimization because they lack the knowledge and generational differences. In these cases, lack of education or access to digital could play a factor whereas outcomes like the chance of becoming a victim and reporting cybercrimes could be a risk for individuals.

The research methods used in these journals vary; you could use quantitative approach to conduct this research. Using surveys and questionnaires for people who have been victims of cybercrimes and for people who have more experience when technology collects quantitative data on victimization rates or user behavior. They could also test and do an experimental simulation of phishing to get a better analysis of age groups that are being targeted and their behavior while going through. For example, researchers can target a group of small children who play video games and figure out a way to get them to buy something from the game. Then they hack into their gaming system for credit card information to see if their security system is strong. Some might have strong systems, others might not. In theory you would think parents have strong supervision of what their child does, but that is not always the case (Cheng et al.).

From our class lecture the formal social control talks about laws and polices you are not allowed to be broken, or consequences will follow. Committing any cybercrime is illegal, but most people get caught, which is unfortunate. Also, The Big 5 Personality Theories can play a part in the victim's actions. For example, the victim's openness. It is easy to become curious about things that you see if you get a message from your bank saying that you have been charged $25 for a subscription you may have, but that message may have a link or a number to call to get it fixed. Most people would click that link or call the said number can then they fell into the trap of being attacked by hackers. Hacker can get a lot of information just from you by clicking a link. Therefore, not answering the message or contacting your bank directly would be the best option.

Challenges faced by marginalized groups like children or ages 65 and up also interact with cybersecurity. For example, low-income populations may be more vulnerable to cybercrime because they lack access to current software, lack of knowledge or lack of a strong security system. "Low-income users are most likely to use older devices that are no longer supported with regular software update patches, and they are least likely to be willing or able to pay for the airtime to download updates" (Cyber Resilience). Problems may make immigrants more vulnerable to phishing schemes. Over time people who are less fortunate can learn how the cyber world works and the pros and cons.

In conclusion, these studies have an important impact to society to identify what are the behaviors and characteristics that make individuals victims but cybercrimes. They help researchers develop preventative measures that shed light on the ways in which social sciences impact cybercrime and increase public understanding of the human aspect of online dangers.

"The Role of Social Science in Cybersecurity Analysis | Azariahpugh." *Odu.edu*, 29 Apr. 2025, sites.wp.odu.edu/azariahpugh/2025/04/29/the-role-of-social-science-in-cybersecurity-analysis/. Accessed 28 Sept. 2025.

Cheng, Cecilia, et al. "Individual Differences in Susceptibility to Cybercrime Victimization and Its Psychological Aftermath." *Computers in Human Behavior*, vol. 108, July 2020, p. 106311, https://doi.org/10.1016/j.chb.2020.106311.

"Cyber Resilience Must Focus on Marginalized Individuals, Not Just Institutions." *Carnegieendowment.org*, carnegieendowment.org/research/2023/03/cyber-resilience-must-focus-on-marginalized-individuals-not-just-institutions?lang=en.