Jacob Pelletier

Professor T. Woodbury

CYSE201S - Spring 2025

27 April 2025

Social Science for Ethical Hackers.

Ethical hacking is often thought as a technical skillset that operates in a black and white manner. This however is not fully accurate. The reality of the profession is that ethical hackers heavily rely on their understanding of human behavior. Social science research and principles are critical when it comes to ethical hackers ability understand how people think and behave in order to predict the motives for cybercrime. Additionally, it is important to understand some of the social factors or theories that may influence individuals to commit crimes. When in comes to any type of crime prevention, social science is a key element in being successful. In regards to ethical hacking, specialist must be able to follow current social trends, events, and politics to effectively think and function as a cybercriminal.

There are many ways that social science research contributes to ethical hacking. Psychological theories such as the Rational Choice Theory, General Strain Theory, Social Learning Theory, etc, help ethical hackers create realistic strategies that will be not only believable, but also successful in creating a breach in security. Additionally, sociology gives ethical hackers insights into how organizational culture and societal norms can influence cybersecurity practices within specific organizations. It is extremely important for ethical hackers to have a strong foundation of knowledge regarding these dynamics in order to predict how cyber criminals might find or create weak points within the human firewall element of security.

In addition to the human behavior focused knowledge, it is important for ethical hackers to understand societal factors such as race, economic status, age, religion, education level, etc. Historically, marginalized communities are more likely to be targeted by cybercriminals. An example of this would be blackmail or "failure to respond" scams targeting elderly people due to their potential lack of awareness in regards to cybercrime. It is important for ethical hackers t to understand that cybersecurity is often influenced by existing social inequities. A strong understanding of these societal issues through the use of research is key in understanding how cybercriminals think and predict where they might focus their efforts.

Ethical hackers have a dynamic field that requires constant reevaluation based on how society functions. Technology is ever evolving, and though this plays a vital role in efficiency and convince in our daily lives, it also creates more opportunity for cyber crime to occur. For ethical hackers, the challenge is to stay current in not only the technology field, but also social trends as well. It is obvious that we utilize technology for things such as banking, medical records, personal communication devices and social media engagement. However, the depths of where technology is being used in modern society is rapidly growing. For example, now household appliances can be linked to other applications such as Alexa and google assistant. Those platforms are often times linked to things such as stored payment methods, emails, contacts and personal demographic information. As a ethical hacker, it is important to understand that the methods of manipulating technology for the purpose of cyber crime is rapidly growing along with technology.

In conclusion, though ethical hacking is a technical profession, it is strongly related to social science principles and research. Understanding human behavior, societal trends, and social class is detrimental in hackers effectiveness in preventing cybercrimes.

Works Cited

Gangadharan, Seeta Peña. “Digital Inclusion and Data Profiling: Marginalized Groups' Access to and Control over Data.” *Telecommunications Policy*, vol. 41, no. 7–8, 2017, pp. 709–719, https://doi.org/10.1016/j.telpol.2017.05.002.

Holt, Thomas J. “Examining the Role of Technology in the Formation of Deviant Subcultures.” *Social Science Computer Review*, vol. 31, no. 2, 2013, pp. 165–178, https://doi.org/10.1177/0894439312452990.

Noble, Safiya Umoja. *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press, 2018.