Hacker Profiling

Richard W. Young

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Matthew Umphlet

March 29th, 2024

Hacker Profiling

The bare bones definition of hacking is gaining unauthorized access to data in a system or a computer. It has been difficult for law enforcement and researchers to study the motives behind what pushes an individual to hack hardware and software. Still, some accurate theories can be made with applying social science principles, different research strategies, and raw data from hacking convictions.

While every hacker is different, researchers can profile them with different principles of social science like social change, social interaction, and socialization. Social change implies that over time, societies evolve through technological advancements, cultural shifts, and demographic changes. Technology and networking advancement could have influenced a wave of next-generation hackers that may have different motives from hackers before. Socialization refers to how family, friends, media, and education mold the ethics and beliefs of someone. Since hacking is an interdisciplinary study of computer science and criminology, one doesn't fall into hacking but spends years learning about it individually or from peers. Social interaction refers to how individuals communicate and interact with one another. If a person surrounds themselves with hackers constantly, that person may be inspired to join them as a social norm, status, or role.

The motive of the research conducted in this article is to create accurate theories as to what drove individuals to engage and succeed in criminal hacking and if they tend to hack alone or in groups. This research also analyzes if there is a relationship between the age, nationality, and gender of convicted hackers and the cyber crimes they commit. To find these possibilities, researchers used "T-tests", "Chi-Squared Tests", and "Logistics tests" with the raw, public data they collected from the United States Department of Justice Computer Crime and Intellectual

Property Section. Gertenfeld, J. (2023) explains that 122 USDOJ CCIPS reports were reviewed and analyzed for this research.

Although the results of this study could help investigators with future incidents, hackers are extremely diverse and hard to study because there are so many different types of them. Like how white, gray, black, and red hat hacker labels deal with the legality of the hacking they do, Gertenfeld, J. (2023) explains that novices, students, cyberpunks, old guards, insiders, petty thieves, professionals, nation states, hacktivists, digital pirates, online sex offenders, crowdsourcers, and crime facilitators are different classifications hackers can have. Different labels and classifications are pinned to hackers which can warp the public's perception of them and turn them into a marginalized group. Speaking of marginalized groups, the groups that are targeted the most by hackers are small to medium-sized businesses and critical infrastructure organizations. Medium-sized businesses are key targets because they most likely lack the cyber security that an organization may have and label them as an easy target. Larger organizations like government, banks, and healthcare are harder targets because they may have cyber security but have larger amounts of valuable data and funds to be extorted.

By utilizing a few principles of social science and different research methods to gather and analyze data on hackers, researchers can determine if personal characteristics can be linked to the cybercrime they commit. This research contributes to society by equipping law enforcement and researchers with a better general understanding of the attacker side of a cybercrime.

References

Gertenfeld, J. (2023). Understanding the connections between hackers and their hacks: Analyzing USDOJ reports for hacker profiles. *International Journal of Cybersecurity Intelligence and Cybercrime. (6)*1, 59-76. https://doi.org/10.1093/cybsec/tyz003