Alexandria Proctor

Instructor Diwakar Yalpi

CYSE 201s

9 April 2025

Ethical Hacking

BLUF: Ethical hackers use knowledge from social science, like psychology, sociology, and criminology, to better understand human behavior, identify system weaknesses, and help protect all types of people online. These skills are important for helping vulnerable groups and making sure cybersecurity is fair and safe for everyone.

Introduction

Ethical hacking is when a cybersecurity professional is hired or given permission to try and find weaknesses in a company's computer systems. These professionals think like hackers, but instead of breaking into systems for fun or money, they help organizations protect themselves. Ethical hackers need more than just technical skills. They must also understand how people think, act, and make decisions. That's where social science comes in. Social science includes psychology, sociology, and criminology. These areas of study help explain human behavior, social patterns, and the reasons why people commit crimes.

Understanding Human Behavior Through Social Science

Ethical hackers use psychology to understand why people often fall for scams or forget to follow security rules. For example, people are more likely to click on emails that look familiar or important, even if they're fake. Knowing this, ethical hackers can better test email systems to make sure they're protected against phishing (Identity Management Institute, 2023). Sociology helps ethical hackers understand how social groups, peer pressure, and community norms affect behavior online. For instance, if everyone in a workplace reuses the same password, others may think it's okay to do the same. Criminology gives insight into why people commit cybercrimes. Some attackers do it for money, others for attention, or even political reasons. Understanding these motivations helps ethical hackers predict what kinds of attacks might happen and how to stop them before they start (IBM, 2023).

How Ethical Hackers Use Social Science Every Day

In their daily work, ethical hackers rely on social science to help them think like both users and attackers. Human behavior is often the weakest part of a security system. People forget passwords, fall for scams, or accidentally download harmful files. Ethical hackers use what they know about human error to design better systems and test how likely people are to make certain mistakes. They also study how people react under stress or pressure, which helps them create real-world simulations to test system safety. When looking at threats, ethical hackers use psychology and criminology to guess how real attackers might try to trick users. For example, if a company is going through layoffs, hackers might send fake emails pretending to offer job help. Ethical hackers use that knowledge to run fake tests and show the company where it's vulnerable.

Ethical hackers also use digital forensics, which is the process of studying digital evidence after an attack. They look at things like login history, file changes, and user activity to figure out what happened. This process is a lot like how criminologists study crime scenes.

Using Research in Ethical Hacking

Ethical hackers follow research methods to find the truth. They create hypotheses, or educated guesses, about what could go wrong and then test those ideas through controlled experiments. For example, they might believe that employees are more likely to click a phishing link if it looks like it's from their boss. To test that, they send a fake email and see how many people fall for it. They collect data on who clicked, how quickly they responded, and what action they took. This helps them understand behavior and suggest better security training (IBM, 2023). Just like in social science, ethical hackers study patterns and use evidence to make informed decisions.

Protecting Marginalized Communities

Cybersecurity doesn't affect everyone equally. Marginalized groups, such as low-income individuals, people with disabilities, or those with limited internet access may not have the same tools or knowledge to protect themselves. These communities are more likely to be targeted by scams, misinformation, or privacy violations. Ethical hackers can help protect these groups by designing systems that are simple, safe, and easy to use. They also help nonprofit organizations and small businesses that serve these communities, which often don't have big security budgets. According to the CyberPeace Institute (2023), ethical hackers sometimes volunteer their skills to help these organizations stay protected. By thinking about fairness, accessibility, and digital rights, ethical hackers make sure their work includes everyone.

Conclusion

Ethical hacking is about more than just breaking into systems, but also understanding how people behave and building better defenses. Social science plays a huge role in this work. Psychology helps ethical hackers understand how people think. Sociology explains how group behavior influences choices. Criminology shows why cybercriminals act the way they do. By using these ideas, ethical hackers protect people and systems more effectively. They also make sure that cybersecurity is fair and safe for those who need it most. As the digital world keeps growing, ethical hackers will continue to rely on social science to solve problems, prevent

Works Cited

IBM. (2023). *Hacking the mind: Why psychology matters to cybersecurity*. https://www.ibm.com/think/insights/hacking-the-mind-why-psychology-matters-to-cybersecurity

CyberPeace Institute. (2023). *Cyber-poor, target-rich: The crucial role of cybersecurity in nonprofit organizations*. https://cyberpeaceinstitute.org/news/cyber-poor-target-rich-the-crucial-role-of-cybersecurity-in-nonprofit-organizations/

Identity Management Institute. (2023). *Psychology of Cybersecurity and Human Behavior*. https://identitymanagementinstitute.org/psychology-of-cybersecurity-and-human-behavior/