Elijah Bernal

Professor Yalpi

CYSE 201S

April 11, 2025

Career Paper

Introduction

An ethical hacker is a cybersecurity expert who uses their hacking skills for good. Ethical hackers use the same techniques a regular hacker would use, but they have permission to do so. The job of an ethical hacker is to find vulnerabilities in security systems so that they can be fixed as soon as possible. In order to do well in the field of cybersecurity, ethical hackers must use principes from social sciences.

Social Engineering

Social engineering is a big part of ethical hacking. Social engineering is the act of tricking somebody into giving away private information (Poston). Ethical hackers use social science to understand how people think, feel, and act. Knowing these important things helps them do their job much better. Social engineering only works by exploiting people's trust, authority, or sense of urgency (Montañez et al). A common social engineering practice of an ethical hacker is sending fake emails pretending to be someone important. This is a form of a phishing email. For example, an ethical hacker would send an email pretending to be the boss and ask an employee to share passwords. That is a very simple form of a phishing email/social engineering.

Understanding Human Thinking

One must understand how people think in order to do well at ethical hacking. The way people think affects how they respond to cybersecurity threats (Montañez et al). An ethical hacker uses that knowledge to create tests that are a little more realistic. They focus on taking advantage of common mistakes like not paying attention. Focusing mainly on these things helps ethical hackers make more effective security tests (National Academies).

Marginalized Groups

Ethical hacking also has to consider how security issues affect marginalized groups of people. Cybersecurity in general needs to pay more attention to inequalities and biases in technology (National Academies). It is very important to understand how certain security vulnerabilities affect certain groups of people.

Social Science Expert Collaborations

A lot of the time ethical hackers will have co-workers from different fields that work alongside them. These co-workers can sometimes be experts in different fields like psychology or sociology. These people are needed to help ethical hackers understand the “why” behind the things that people do. An example of this would be a psychologist helping an ethical hacker understand why certain people are more likely to fall for cyberattacks then others. On the other hand, a sociologist would be able to explain how an organization’s culture affects their security practices. All of this is done so that ethical hackers can create more effective tests for their organization’s specific needs.

Training

Another way social science ties into ethical hacking is through helping them create educational programs. They use their knowledge of human behavior to create training that teaches people how to be more safe when using the internet. These training programs would be very helpful to teach employees more about cybersecurity and how important it is. Proper training would help employees cut out simple mistakes, like falling for phishing emails or social engineering tactics.

Ethics

Maintaining trust and transparency is important when it comes to the social sciences. Ethical hackers understand this, so they follow rules that make sure they don't cross certain ethical lines that invade people's privacy. Ethical hackers have to get permission for any of the important things that they do.

Conclusion

In conclusion, ethical hackers have to use social science so that they can do their job effectively. Ethical hackers use social science tactics like social engineering at times when needed. They also have to pay attention to how cybersecurity affects marginalized groups. Working with experts from social science fields helps ethical hackers create safe online environments for all types of people.

Works Cited

Montañez, Rosana, et al. "Human Cognition through the Lens of Social Engineering Cyberattacks." *Frontiers in Psychology*, U.S. National Library of Medicine, 30 Sept. 2020, pmc.ncbi.nlm.nih.gov/articles/PMC7554349/. Accessed 11 Apr. 2025.

Poston, Howard. "Ethical Hacking: Social Engineering Basics." *Infosec*, 22 Oct. 2019, www.infosecinstitute.com/resources/hacking/ethical-hacking-social-engineering-basics/. Accessed 11 Apr. 2025.

"Read 'A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis' at Nap.Edu." *6 Integrating Social and Behavioral Sciences (SBS) Research to Enhance Security in Cyberspace | A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis | The National Academies Press*, nap.nationalacademies.org/read/25335/chapter/10. Accessed 11 Apr. 2025.