Ethical hackers or White hat hackers are cyber security professionals that are very savvy in understanding, testing and gaining access to a various systems. Even though this role has a high technical aspect to it, another aspect that is extremely important is the social sciences behind it. Ethical hackers need to know not only the software and hardware of the system they are testing but they also need to understand the mindsets and idiosyncrasies of the people utilizing these systems. Having a deep understanding of this assists them in finding vulnerabilities in a plethora of systems and or processes. In this paper I will examine how professionals in this field rely on the social sciences principles and social science research methods, application of key concepts, the relationship between hackers and marginalized groups and how careers are related to society today.

Social sciences principles

Another name for Ethical Hackers is Penetration testers. Some Ethical Hackers are given the keys to the kingdom such as a password to one account, and they test the internal security of different networks or devices in one organization by trying to pivot through the system laterally. In some organizations they are hired to find a way into the client's network from outside of the network by any means necessary yet this doesn't mean in a convoluted technical way. They can gain access from social engineering and exploiting specific targets or organizations. Social engineering is the exploitation or the hacking of human behavior rather than technical vulnerabilities. 98% of cyber-attacks rely on social engineering (Kidd & Raza, 2024). Ethical hackers rely on the social science principles and behavioral sciences such as psychology to figure how to create a cyber-attack geared towards specific targets.

Determinism is another social science that can be utilized in the defensive side of ethical hacking. Incorporating determinism with the monothetic model can create a precise view and understanding of an organization's repeated failures to avoid cyber threats. Analyzing that data will inform the hacker how to properly make a structured cyber security program training or prevention program. With this data programs can be tailored by age, profession, and job title to be dispersed through the organization and selectively produce increases in the observation of cyber-attacks and how to avoid them.

Social Science research methods.

These intelligent security specialists also do their own type of research as a preliminary task before crafting an exploit. Empirical research is key for white hat hackers because hard data that's derived from surveys, phishing tests, network traffic analysis and observational data is essential in the reconnaissance step in crafting a successful exploit. It is also extremely important for the defensive posture of the system. Ethical hacking is in the business of both offensive and defensive measures to test the hardening of a system. Also to test if such vulnerability fixes actually work.

Key Concepts

On the other tip of the spear, defensive mechanisms and processes can be researched, socially engineered and created to protect the users from system intrusion. Cyber security awareness training and courses can assist in this effort tremendously. The concept of Human-system Integration HSI engages human factors including cognitive implementation to design a training tailored for success. According to Brown

and Magdira (2025) recently only 44% of people always check their messages for signs of phishing. In today's time phishing has evolved from just email phishing to SMS and Voice phishing attempts. With this empirical data combined with HSI a robust training plan can be created and hopefully increase the scrutiny of which one checks their messages for a cyber-attack. Something as simple as changing the navigation within the user interface can provide an increase in spotting fake channels of communication.

Marginalized groups

White hat hackers have an important position in helping and protecting marginalized groups. They use their skill to fix, identify, notify people of the vulnerabilities found and training for people and organizations. Many white hack hackers volunteer in lower income areas where cyber-attacks disproportionately affect their community compared to other socioeconomic groups. 13% of Latinx and 14% of Black consumers were victims compared to their white counterparts (Rodriguez, 2024). One could assume that cyber training and awareness is not as prevalent in lower income areas just like the typical lack of food, shelter and Transporation. Ethical hackers volunteering and fostering a good environment for underprivileged people to learn is a relationship that can help decrease the number of cyber-attacks globally.

Ethical Hacking and society today.

Ethical hacking plays a crucial role today. Over the past 2 decades the cyber front has grown so much and so much of our PII and financial information is online too that there is a need for White hat hackers. As cyber space grows so will the threat vectors, sophistication and number of cyber-attacks by foreign state and malicious

actors. A huge portion of the typical Americans life today is done utilizing the internet. We order food, clothes, communicate with loved ones, attend school and even work online from our homes. System owners aggregate an immense amount of data and leave a trail of digital dust that could be trailed and accessed if the right measures aren't in place. Without the vulnerability research of ethical hacking so many more victims could fall victim to financial losses or privacy leakage.

Conclusion.

In conclusion I find the role of ethical hacking a very interesting and lucrative career within the cyber security field. The vulnerability analysis that comes from ethical hacking is crucial and important to the entire world of network systems. It is an ever-changing landscape, and it will only become more of a necessity in the future. Ethical hacking is a scrupulous necessity needed in the digital realm.

References

Rodriguez, Y. (2024, October 18). *Report: Black and Latino consumers twice as likely to be targets of online financial fraud*. Texas Standard. Retrieved April 12, 2025, from https://www.texasstandard.org/stories/consumer-reports-online-financial-fraud-black-latino-communities-phishing-rates-protection/

Kidd, C., & Raza, M. (2024, August 6). *What are social engineering attacks? A detailed explanation | Splunk*. Splunk. Retrieved April 12, 2025, from https://www.splunk.com/en_us/blog/learn/social-engineering-attacks.html#:~:text=98%25%20of%20cyberattacks%20rely%20on%20social%20engineering.

Brown, A., & Magdirila, P. (2025, March 31). *Cybersecurity Awareness: The Human Factor In Phishing Attacks*. AvePoint. Retrieved April 12, 2025, from https://www.avepoint.com/blog/protect/phishing-attacks

Derek D. Hillman
04/13/2025

Career Paper Hackers
United