*Cybersecurity Professional Career Paper*

Niaya Fuller

Old Dominion University

November 16, 2025

For Cybersecurity, there are many career paths one can take. According to the NICCS, one could be a Chief Security Officer, Network Security Analyst, or a Network Defense Technician. - With the high-speed growth of technology, Cybersecurity is very important in not only managing the security of the systems, but it is also crucial in protecting valuable data in an ever-evolving world. The purpose of this paper is to highlight the importance of a specific career: Ethical Hacking.

# Social Science Principles

For ethical hacking, there are many social science principles that are applied or referenced. One of the main principles is understanding human behavior, not just on the hacker side but on the victim side as well. Is it for fun? For money? These are important questions to know where to pinpoint places hackers will target. To be an ethical hacker, however, one must follow hacking law, as mentioned in Module 12. They would be going into systems, just as hackers would, and with

that comes the responsibility of not irresponsibly breaching any laws or regulations while said systems are vulnerable.

### Application of Key Concepts

In the career of ethical hacking, there are many ways those key concepts are applied. Similar to hacking law, ethical hackers must follow a code of ethics. As Johansen mentions as an example code of ethics, one must determine the sensitivity of information, must not go past the limits of the client, maintain transparency, and never disclose confidential information to others. Another concept that is applied is the understanding of human behavior. One way that is taken into account is during one method of hacking: Social engineering. To effectively social engineer, one must understand people in order to develop a quick relationship and slowly and meticulously manipulate the persons to give confidential information. One has to understand the different personalities of their victims so they can take different approaches to get the information, as well.

## Marginalization and Connection to Society

Technology, as a whole, is becoming intertwined with society at a pace one can't necessarily measure. As a response, cybersecurity is needed more than ever to keep people's and business' information safe. Ethical hacking is just that, where one would find vulnerabilities in systems before anyone malicious did first, ensuring that there are as little vulnerabilities for them to exploit. By making companies aware of these vulnerabilities, marginalized communities and people would be protected more from malicious hacking. Marginalized groups are mainly the target of these attacks, with Jarett and Roberts mentioning that small businesses, people of color, and hospitals are the focus. Oftentimes these businesses or people either are under financial

strain that leaves them unable to properly protect themselves, are using third party services that are at risk of attacks or are simply unaware of the vulnerabilities in their systems. This is why ethical hacking is important, especially in an age of growing technological use. It would aid companies in keeping not only themselves, but customers and their information safe.

## References

*Cyber Career Pathways Tool*. (2025, September 5). National Initiative for Cybersecurity Careers and Studies. https://niccs.cisa.gov/tools/cyber-career-pathways-tool?quiet=1

*Cyberattacks disproportionately affect vulnerable communities. Is this an opportunity for impact investors? – SJF Ventures*. (2024). Sjfventures.com. https://sjfventures.com/cyberattacks-disproportionately-affect-vulnerable-communities-is-this-an-opportunity-for-impact-investors/

Johansen, R. (2023, October 13). *Ethical Hacking Code of Ethics: Security, Risk & Issues*. Panmore Institute. https://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues

Yalpi, D. (n.d.). *CYSE 201S Module 12*.