Cybersecurity: It's Not Just About Hackers and Passwords

Hussein Al Saffar

Department of Cybersecurity, Old Dominion University

CYSE201S: Cybersecurity & Social Science

Professor Matthew Umphlet

June 28, 2025

Cybersecurity: It’s Not Just About Hackers and Passwords

When I first began studying cybersecurity, I realized how many misconceptions I had carried with me, most of them shaped by popular culture, news headlines, or a limited understanding of how digital threats work. One of the first ideas I had to let go of was the stereotype that all hackers are criminals, usually portrayed in movies as mysterious figures in hoodies typing furiously in the dark. I learned that the term “hacker” simply refers to someone who understands how systems work and can manipulate them—sometimes for malicious purposes, but often for good. Ethical hackers, or “white hats,” play a vital role in cybersecurity by helping companies identify and fix vulnerabilities before real attackers can exploit them.

I also assumed that having antivirus software installed meant I was fully protected from cyber threats. That belief quickly fell apart once I started learning about how sophisticated and varied cyberattacks can be. Antivirus is helpful, but it’s only one part of a much broader defense strategy that includes firewalls, regular system updates, secure configurations, and—perhaps most importantly—user awareness. Another misconception I had was that hackers primarily go after large corporations or wealthy individuals. I thought, “Why would anyone want to hack me?” But I soon realized that cybercriminals often target everyday people because they tend to have weaker defenses and can be tricked into revealing personal information or paying ransom. In fact, small businesses and individuals are often the most common targets of phishing and ransomware attacks.

Another belief I had was that strong passwords were the ultimate line of defense. While strong passwords are important, I learned that they can still be stolen, guessed, or exposed in data breaches. This is why multi-factor authentication (MFA) has become such an essential layer of protection it adds an extra step that significantly increases security. One of the more surprising realizations I had was that cybersecurity isn’t just about technology or computer science. I had thought it was all about coding, encryption, and complex systems, but I’ve since learned that human behavior plays a huge role.

Social engineering, phishing, and insider threats rely more on manipulating people than on bypassing technical barriers. It made me understand that cybersecurity is as much about psychology and communication as it is about machines.

Finally, I used to think that if something wasn’t connected to the internet like an offline computer or an isolated system it was completely safe from attack. But I’ve learned that even “air-gapped” systems can be compromised, often through physical means like infected USB drives or through the actions of careless or malicious insiders.

This taught me that no system is ever 100% secure, and that every environment needs layered defenses and strict policies to stay protected. Reflecting on these misconceptions has shown me just how complex and constantly evolving the world of cybersecurity really is. It’s not just a technical field it’s a human one. The more I learn, the more I understand how important it is to think critically, stay informed, and never assume that any one tool or habit is enough on its own. Cybersecurity is about building a mindset of continuous learning and cautious awareness, and that mindset will stay with me both online and offline.

References

Greenberg, A. (2016, April 6). *Hacker lexicon: What is the difference between white hat, gray hat, and black hat hackers?* Wired. https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/

Coker, J. (2025, March 11). 95% of data breaches tied to human error in 2024. *Infosecurity Magazine.* https://www.infosecurity-magazine.com/news/data-breaches-human-error/