

Journal Entry Six

Nicholas Duggins

Matthew Umphlet

07/05/2026

Journal Entry Six

Before I started learning about the connection between social science and cybersecurity, my idea of digital threats was mostly shaped by movies and what you see online. I honestly thought hacking worked like it does in Hollywood for fast typing, dark screens, and someone breaking into a “mainframe” in a few minutes just because they’re really smart. I also had a pretty limited understanding of what cyberattacks actually do. I figured most security breaches were just minor issues like a frozen computer, a lost file, or maybe some temporary inconvenience that gets fixed quickly.

As I went through my coursework, I realized how wrong those assumptions were. Real hacking isn’t fast or flashy; it’s slow, planned, and very strategic. A lot of it isn’t even about writing code at high speed. Instead, attackers spend a lot of time researching their targets, gathering information, and using psychology to manipulate people into making mistakes. It’s more about understanding human behavior and taking advantage of it than anything else. That part really changed how I look at cybersecurity, because it showed me that people are often the weakest point in a system, not the technology itself.

I also learned that the effects of cybercrime go way beyond what I originally thought. These attacks can disrupt entire organizations, including schools and universities, damage trust between companies and clients, and even cause real harm to people through things like financial fraud or targeted scams. What I used to think of as “just a computer problem” is something that can ripple out into real-life consequences for communities and individuals. Overall, this course helped me understand that cybersecurity isn’t about movie-style hacking. It’s about patience, strategy, and understanding human behavior, and that completely changed how I view digital safety.

Journal Entry 8

Nicholas Duggins

07/12/2026

Journal Entry 8

After watching the videos, I realized how much movies and television influence the way people think about cybersecurity. Before taking this class, I probably would have believed some of the things shown in movies. Most media portray hackers as people who can break into any computer system in a matter of seconds just by typing really fast on a keyboard. While these scenes make movies more exciting, they are usually not realistic.

One thing I learned from this course is that real hacking is much more complicated than what we see in movies. The experts in the videos explained that cyberattacks often take a lot of planning, research, and patience. Instead of instantly breaking into systems, many hackers take advantage of human mistakes through phishing emails, weak passwords, or social engineering. This connects to what we have been learning in class about the human element of cybersecurity and why people are often the biggest vulnerability.

My understanding of cybersecurity has definitely changed over time. Before learning about it, I thought hacking was mostly about technical skills and writing complex code. Now I understand that cybersecurity is not just about technology. It is also about human behavior, policies, training, and awareness. I also noticed a difference between older and newer media. Older movies often showed unrealistic hacking scenes with flashy graphics and impossible computer capabilities. Newer movies and shows still exaggerate some things, but they do a better job of showing real cybersecurity concepts like phishing, malware, and data breaches. Overall, these videos showed me that media can create misconceptions about cybersecurity, but newer portrayals are starting to become more realistic as technology becomes a bigger part of everyday life.

Journal Entry 10 Part 1

Nicholas Duggins

07/17/2026

Journal Entry 10 Part 1

The video What Does a Cybersecurity Analyst Do? Salaries, Skills & Job Outlook showed a lot of the day-to-day responsibilities of a cybersecurity analyst, but what stood out to me was how much of the job revolves around people. Most cyberattacks are not just about technology. They take advantage of human behavior. Things like phishing emails and social engineering scams work because attackers know how to manipulate trust, emotions, and people's willingness to help. A cybersecurity analyst has to understand these human factors just as much as they understand computers and networks.

Another social theme I noticed is communication. Analysts must work with employees, managers, and other departments to keep systems secure. Sometimes security policies can be frustrating or inconvenient, so analysts need to explain why those policies matter and help create a culture where people take cybersecurity seriously. In a lot of ways, they are educators as much as they are technical experts.

The video also showed that cybersecurity analysts must be adaptable because threats are constantly changing. New scams, malware, and attack methods appear all the time, which means analysts must continue learning and educating others. Their ability to identify risks and respond quickly can help prevent major security incidents that could impact an entire organization.

Overall, this video reinforced the idea that cybersecurity is not just about protecting technology. It is about protecting people and understanding how human behavior affects security. The human element is often the weakest link, which is why cybersecurity analysts play such an important role in helping organizations stay safe.

Reference:

GRC For Mere Mortals. (2023). What does a cybersecurity analyst do? Salaries, skills & job outlook [Video]. YouTube. <https://www.youtube.com/watch?v=iYtmuHbhmS0>

Journal Entry 10 Part 2

Nicholas Duggins

07/17/2026

Journal Entry 10 Part 2

After reading Social Cybersecurity: An Emerging National Security Requirement, I realized that cybersecurity is much more than protecting computers and networks. Beskow and Carley (2019) explain that modern threats often target people instead of technology. Rather than hacking systems directly, attackers use social media, misinformation, and psychological tactics to influence how people think, act, and make decisions. This idea of "cognitive hacking" was one of the most interesting parts of the article because it shows how human behavior can be used as a weapon.

One thing that stood out to me was how foreign governments and other groups can use social media platforms to spread false information and create division within a country. The article explains that these actors use bots, algorithms, and coordinated campaigns to manipulate public opinion and weaken trust in institutions. In today's world, information can spread almost instantly, which makes it easier for bad actors to influence large groups of people without ever being physically present.

The BEND model discussed in the article was also interesting because it shows the different ways information can be used to shape beliefs and behaviors. It helped me understand that cyber threats are not always technical attacks. Sometimes the goal is simply to confuse, distract, or divide people.

As an Army veteran, I found the national security aspect especially important. The article reinforced that protecting a country now requires more than securing military systems and government networks. It also requires protecting citizens from manipulation and misinformation. Overall, this article showed me that cybersecurity and social science are closely connected. Understanding human behavior is just as important as understanding technology when it comes to defending against modern cyber threats.

Reference

Beskow, D. M., & Carley, K. M. (2019). Social cybersecurity: An emerging national security requirement. *Military Review*, 99(2), 117–127. <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/>