

Journal 1: Are there certain areas that you want to focus your career on?

As I've learned about cybersecurity, I've found that many aspects of this job interest me such as conducting audits that will determine security violations or vulnerabilities, implementing security technology, and developing firewalls for networks. The aspects of those jobs are very interesting and would motivate me to work rather than areas of the jobs that would require me to teach employees throughout the company about security policies and practices.

Journal 2: Explain how the principles of science relate to cybersecurity.

Determinism: this term suggests that events have causes that happen due to the causes. We can use determinism to analyze the causes of security breaches or incidents. If we understood factors for cyber threats, cybersecurity specialists could use measures to prevent them.

Relativism: This term means that knowledge and truth are influenced by various factors. With Cybersecurity, relativism can relate to viewpoints for privacy and security. Perspectives on these can be very important for organizations.

Objectivity: This term refers to the unbiased analysis of evidence. While working in cybersecurity, objectivity is very important for conducting different investigations and analyzing incidents that occurred.

Parsimony: This term suggests that explanations should be kept simple. Within the cybersecurity world parsimony is widely used to avoid complexity to identify security vulnerabilities.

Skepticism: This term means to question and critically evaluate claims and evidence. In cybersecurity, keeping a skeptical mind helps professionals make informed and correct decisions.

Ethical Neutrality: This suggests that research should be conducted without any judgement or bias. This is important for any field; it is very important to keep a professional view and mindset on the job.

Journal 3: How might researchers use the information on [PrivacyRights.org](https://www.privacyrights.org) to study breaches?

With the information on this website, researchers can determine what types of hacks are highly used, which states have a higher number of breaches, and which organizations or individuals are more likely to be attacked. Within this website, we can see that "BSF" are most likely to be

attacked which is financial services, banking, and insurance services. This is due to the amount of money that can be taken and used by cybercriminals. From this research, researchers should be able to learn which organizations need more security and how to prevent any intrusions from happening in the future from the previous data recorded.

Journal 4: Review Maslow's Hierarchy of Needs and explain how each level relates to your experiences with technology. Give specific examples of how your digital experiences relate to each level of need.

Maslow's Hierarchy of Needs is a psychological theory that describes human motivation and the different level of needs that Individuals want to fulfill. This hierarchy is depicted with five levels: physiological needs, safety needs, love and belongingness needs, esteem needs, and self-actualization needs.

We can relate these needs to our own digital experiences like:

1. Physiological needs: This is the first level which includes basic needs such as food, water, and shelter. In relation to technology, this represents the need for internet service or devices to fulfill our desires.
2. Safety needs: This is the second level which involves feeling secure. We can relate this to technology by the way we use passwords to protect our accounts and data.
3. Love and belongingness needs: This is the third level which focuses on the need for connection and relationships with others. We can relate this to technology by how technology has made communication and connections way easier around the world through instant messaging and social media.
4. Esteem needs: This is the fourth level which is related to self-esteem, respect, and recognition from others. Technology is related to this due to the creation of social media where a post can receive an amazing amount of likes and attention that can give someone a sense of validation
5. Self-actualization needs: This is the highest level which represents personal growth, realizing potential, or pursuing goals and aspirations. Advancements in technology in the current world has made it easier for individuals to build their minds through tutoring or online courses.

Journal 5: Review the articles linked with each individual motive. Rank the motives from 1 to 7 as the motives that you think make the most sense (being 1) to the least sense (being 7). Explain why you rank each motive the way you rank it.

1. Multiple Reasons: This is ranked at the top due to how many different factors are usually needed for someone to pursue a cybercrime.
2. For Money: This is second due to many people believing they can get away with easy money through a cybercrime.
3. Revenge: Many individuals are unaware of how secured the cyber world is and will commit revenge crimes. For individuals to commit a crime, the reward to the crime must outweigh the punishment and revenge outweighs many punishments.
4. Political: Many crimes are committed due to politics, however I believe that its ranked in the middle of this list due to the other factors listed.
5. Recognition: Most cybercriminals mask their identity when committing crimes such as the famous cybercriminal group Anonymous. As their group may be famous their identities remain a mystery.
6. Boredom: I believe that there are many other things that individuals can participate in today's age, this is the reason why I ranked this very low. As this can be a factor, it's not very common due to the amount of activities that are available.
7. Entertainment: As boredom and entertainment are somewhat connected, I ranked this the lowest because I don't believe many people would find committing criminal acts online are entertaining as we live in an age where everyone knows the consequences of these online actions.

Journal 6: How can you spot fake websites? Compare three fake websites to three real websites. What makes fake websites fake?

To spot fake websites, there are many different things to look out for such as:

1. URL: Fake websites have misspelled URLs that contain extra characters that almost imitate legitimate websites.
2. Verify contact information: Real websites use clear contact information such as phone numbers and email addresses, while fake websites don't include this information or have very generic contact information.
3. Website design and functionality: fake websites usually have poor design or low quality websites that include many errors while trying to access it.
4. Unrealistic offers: Fake websites try to trick customers into buying their "products" with their very unrealistic deals they have to get their information.

Fake Websites:

1. CheapIphones.com: this website offers iPhone a very low prices but has a very generic name and doesn't provide any contact information
2. LuxuryBags.com: This website tries to trick a specific audience(women) into buying luxury bags for cheap. This website includes spelling errors and has many functionality problems

3. Freetravel.com: This website has an unrealistic deal of free tickets to different places if a user enters their credentials and information first

Real Websites:

1. Amazon.com: This is a very reputable e-commerce website that has many reviews and a great variety of products. Clear contact information and user-friendly interface
2. Apple.com: This website shows their companies' products, services, and payment options. Well-designed website and secure.
3. Replit.com: An educational and free use website that people can use for their own needs. Has all the contact information, is user-friendly, and has a very functional design.

Journal 7: Review the following ten photos through a human-centered cybersecurity framework. Create a meme for your favorite three, explaining what is going on in the individual's mind. Explain how your memes relate to Human-centered cybersecurity.

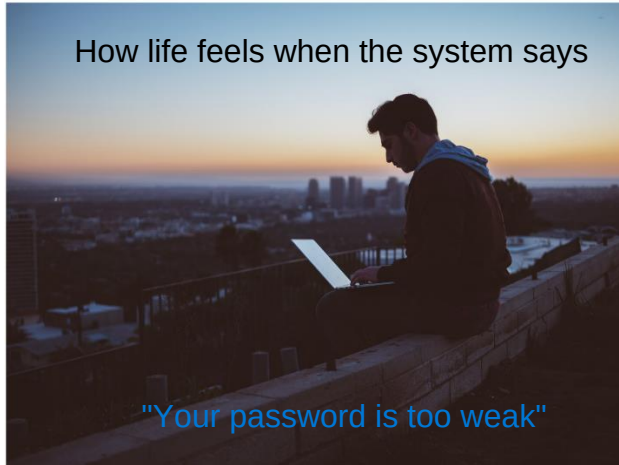
Human systems integration is the way human behaviors influence online privacy and security.

Image 1: This relates to Human-centered cybersecurity because many people make their passwords too easy to guess because they don't want to make anything too complex.

Image 2: This relates to Human-centered cybersecurity because individuals are often targeted by phishing schemes. Learning these different tips and tricks are vital while using the digital world.

Image 3: This relates to Human-centered cybersecurity, ensuring you have proper knowledge over the most common malware attacks or phishing schemes are very important

How life feels when the system says



"Your password is too weak"

When you thought you got accepted



But it was an email from COOGLE

Okay who clicked on the link for the free toaster
this time



Journal 8: After watching the video, write a journal entry about how you think the media influences our understanding about cybersecurity.

I believe that hacking throughout movies is often sped up and exaggerated to get people interested in what is happening in the movie. Often times hacking is done within seconds in movies while it can take weeks of planning and strategies to fully hack something in real life.

Journal 9: Complete the social media disorder scale. How did you score?

What do you think about the items in the scale?

Why do you think that different patterns are found across the world?

I scored three out of nine. Finding out how many people have these problems with social media is very interesting. I didn't know that social media had a great effect over others. I believe that these patterns are found across the world due to the recognition or good feelings that others get when they use social media.

Journal 10: Read this and write a journal entry summarizing your response to the article on social cybersecurity. [Social Cybersecurity an Emerging National Security Requirement \(army.mil\)](https://www.army.mil/article/234567/Social_Cybersecurity_an_Emerging_National_Security_Requirement)

After reading the article on social cybersecurity, I am very concerned and interested in this emerging field to come. While this may be essential to national security, its ability to manipulate human behavior through the use of technology is very concerning. As technology grows, the threats that come with it only grow as well though. Due to this, many countries have made their own cyberwarfare to ensure the protection from any cyberthreats.

Journal 11: Watch this video, as you watch this video, think about how the description of the cybersecurity analyst job relates to social behaviors. Write a paragraph describing social themes that arise in the presentation. [What does a Cybersecurity Analyst Do? Salaries, Skills & Job Outlook - YouTube](https://www.youtube.com/watch?v=...)

In the field of cybersecurity, social themes or behaviors play a huge role in how things operate. Cybersecurity analysts deal with many technical things such as monitoring networks or threats, but they also have to study the behavior of people online. Tricks are used by hackers to get information from people and many factors must be considered when dealing with this and how they operate. Also, social norms from different areas must be considered when dealing with these threats as well.

Journal 12: Read this sample breach letter “SAMPLE DATA BREACH NOTIFCATION” and describe how two different economic theories and two different social sciences theories relate to the letter.

[Glasswasherparts.com .pdf \(dojmt.gov\)](#)

Economic theories:

1. Liability theory: The breach letter is addressing liability, because the company is taking responsibility for the data breach that happens and is informing their customers about it.
2. Information flow theory: The breach letter also reflects information flow theory due to how they are communicating transparently about what happened and will provide more information if needed.

Social science theories:

Parsimony theory: Parsimony theory emphasizes the simplicity and efficiency in explanations and solution. The breach letter had parsimony the way they addressed the problem and told the customers they would assist if need be.

Determinism theory: This theory explains how events and outcomes are shaped by preexisting conditions and causes. In this breach letter, determinism is seen in the events that led up to the breach.

Journal 13: A later module addresses cybersecurity policy through a social science framework. At this point, attention can be drawn to one type of policy, known as bug bounty policies. These policies pay individuals to identify vulnerabilities in a company’s cyber infrastructure. To identify the vulnerabilities, ethical hackers are invited to try exploring the cyber infrastructure using their penetration testing skills. The policies relate to economics in that they are based on cost/benefits principles. Read this article [Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties | Journal of Cybersecurity | Oxford Academic \(oup.com\)](#) and write a summary reaction to the use of the policies in your journal. Focus primarily on the literature review and the discussion of the findings.

This article explores how bug bounty policies are used, and it involves how they pay ethical hackers to find vulnerabilities in a company's cyber infrastructure. The findings in this article show how effective the bug bounty policies are for incentivizing ethical hackers to find vulnerabilities, because of how much it improves organizations security. Many hackers participate in these for no money as well just for bragging rights which helps companies that lack funds.

Journal 14: Adriy Slynchuk has described eleven things internet users do that may be illegal. Review what the author says and write a paragraph describing the five most serious violations and why you think those offenses are serious.

In the article that Adriy Slynchuk writes, he highlights eleven actions that internet users may engage in that could potentially be illegal. In this article, five acts stand out the most that could cause serious online violations. The first one is hacking into computer systems or networks, this can lead to unauthorized access to sensitive information. The second one is engaging in online fraud, this can result in damage to someone's reputation. The third is distributing malicious software such as malware. Sharing copyright material without permission is a serious offense as it violates property rights. Lastly, cyberbullying is a very serious violation as it can cause serious harmful effects on some individuals.

Journal 15: [Digital Forensics | Davin Teo | TEDxHongKongSalon \(youtube.com\)](#) watch this video and think about how the career of digital forensics investigators relate to the social sciences. Write a journal entry describing what you think about the speakers pathway to his career.

In this video, I learned that David transitioned from a field of Accounting into digital forensics. It reminded of me as I transitioned from automotive mechanic to a field of cybersecurity. After watching this video, I am very interested in how they play crucial roles in uncovering and analyzing digital evidence to solve crimes and provide justice. This field requires technical skills and knowledge on humans.