Journal Entry #1

Question: Review the NICE Workforce Framework. Are there certain areas that you would want to focus your career on? Explain which areas would appeal the most to you and which would appeal the least.

Areas That May Appeal the Most to me:

Protect and Defend: I thrive in high-pressure situations and enjoy solving complex puzzles. From reading it I will be at the forefront of cybersecurity incidents, helping organizations recover from and mitigate security breaches.

Securely Provision: After reading about this it seems your shaping an organization's security policies and ensuring compliance with regulations, focusing on security policy and governance can be rewarding. I would be responsible for creating and implementing policies to protect data and systems.

Analyze: I have a analytical mind and enjoy dissecting threats and vulnerabilities. This job youll have to assess systems, networks, and data to identify and mitigate risks.

Areas That May Appeal the Least to me:

Operate and Maintain: Im not particularly interested in the day-to-day management and maintenance of IT systems and infrastructure.

Oversee and Govern: Yes I will be overseeing a lot as a Naval Officer and less in the technical side of the programs. I really like to have more boots on the ground.

Research and Development: I prefer practical, hands-on work over theoretical research, so I find this less appealing.

Journal Entry #2

Question: Explain how the principles of science relate to cybersecurity.

In the field of Cybersecurity the principles of science are very important in understanding, analyzing, and mitigating evolving threats and challenges. The intersection of cybersecurity and science can be looked at from many directions. Here's a couple that stood out to me the most.

Experimentation and Testing

Science relies on observation and data collection and analysis of data. Some examples of this relating to cybersecurity can be network traffic logs, system event record, and attack patterns. These are essential to finding vulnerabilities in a system.

Interdisciplinary Approach
Science often merges knowledge from many disciplines to address complex issues. Cybersecurity merges different fields like computer science, sociology, psychology. Understanding those disciplines for cybersecurity will make you excel in Cybersecurity.

Ethical Considerations
Science has a strong emphasis on ethical conduct and being responsible while conducting research. In cybersecurity. Being in this field you need to adhere to ethical standards , privacy rights, and legal and regulation set by the workplace and state. For example you can't just barge into a workplace requesting information from someone. Thats a invasion of their privacy In conclusion, the principles of science are intertwined with cybersecurity.

Journal Entry #3

Question: Visit PrivacyRights.org to see the types of publicly available information about data breaches. How might researchers use this information to study breaches? Enter a paragraph in your journal.

I believe PrivacyRights.org is a valuable resource for researchers studying data breaches. The publicly available information about data breaches on this site can help be a dataset for various research purposes. Researchers can analyze the data to identify trends and patterns in breach incidents, such as the industries most commonly targeted, the methods of intrusion used, the types of compromised data (such as personal, financial), and the geographic distribution of breaches. This information can help to better understand the cybersecurity landscape, allowing researchers to assess the effectiveness of security measures and recommend improvements where they might see fit.

Journal Entry #4

Maslow's Hierarchy of Needs is a psychological theory that describes human motivation and development in a hierarchical structure, with each level of need building upon the previous one. The five levels, from the foundational to the highest, are physiological, safety, love and belonging, esteem, and self-actualization. Let's explore how each level relates to my experiences with technology, providing specific examples:

Physiological Needs:

In the digital age, technology plays a significant role in meeting basic physiological needs, such as access to food and water. Food delivery apps like Uber Eats and online grocery shopping platforms ensure convenient access to nourishment.
Fitness and health-tracking apps help monitor and improve physical well-being. Devices like smartwatches can track steps, heart rate, and sleep patterns, promoting a healthier lifestyle.

Safety Needs:

Technology enhances personal safety through tools like home security systems and smartphone apps for emergency services. For instance, Ring doorbell cameras provide a sense of security by allowing remote monitoring of one's property.
Cybersecurity measures, like antivirus software and encryption, help protect personal data and financial information, contributing to a feeling of digital safety.

Love and Belonging:

People can connect with friends and family using social media platforms like Facebook and Instagram, which promotes a sense of belonging and makes it easier to communicate even when people are separated by great distances.
People have the chance to make romantic connections and friendships online thanks to dating apps like Tinder and Match.com.

Esteem Needs:

Through tools for self-expression and validation, technology can improve self-esteem. Positive feedback and a sense of accomplishment can come from blogging, vlogging on YouTube, or sharing original content on websites like TikTok.
Professional networking sites like LinkedIn enable people to highlight their abilities, accomplishments, and achievements, enhancing their self-worth and career development.

Self-Actualization:

By granting access to educational resources and courses, online learning platforms like Coursera and edX enable people to pursue their passions and interests and promote self-actualization. The immersive experiences provided by virtual reality and augmented reality technologies can assist people in their quests for self-actualization by allowing them to explore new horizons, hobbies, or even travel to locations they may never physically visit.

In conclusion, technology has ingrained itself into our daily lives and become a tool for meeting the different levels of needs described in Maslow's Hierarchy. Technology plays a significant role in enhancing our wellbeing and personal development in the digital age, from fostering self-actualization to addressing fundamental physiological needs.

Journal Entry 5:

1. For Money (1): This motive makes the most sense as cybercriminals often seek financial gain through activities like ransomware attacks, identity theft, and online fraud. I do see Bitcoin on the pictures for this article and its crazy to think this is all tax free and untraceable. Money is a universal motivator, and cybercrime can be highly profitable.

2. Political (2): Political motivations can make sense, as hacktivists may target individuals or organizations to further political agendas. These attacks aim to influence policies or disseminate information, making them a relatively understandable motive.

3. Revenge (3): Revenge-driven cybercrimes, where people seek retribution against someone or an organization, have a clear motive even though they may not justify the actions. For example revenge porn, and now people are able to create deepfakes of people from speeches to other people and too putting people's faces on pornographic images.

4. Entertainment (4): Some individuals engage in cybercrimes purely for entertainment or to test their hacking skills. While it may not make sense from an ethical standpoint, it's a motive that can be understood in the context of thrill-seeking behavior. Its kind of stupid as there is many other things you could be doing for fun.

5. Recognition (5): Seeking recognition by gaining notoriety in the hacking community or among peers can motivate cybercriminals. They may want to prove their skills or establish a reputation, making this motive somewhat sensible in their subculture.

6. Multiple Reasons (6): Many cybercriminals have a combination of motives, which can include any of the above. This mixed motive category is complex, as individuals may have financial, political, or personal reasons for their actions.

7. Boredom (7): Boredom is the motive that makes the least sense. While it may explain some low-level cyber mischief, it's hard to justify causing harm to others and potentially facing severe legal consequences simply out of boredom.

Journal Entry #6

Question : Can you spot three fake websites and compare the three fake websites to three real websites, plus showcase what makes the fake websites fake?

Like we said in class, we aren't actually looking for fake websites. So here some general ways to identify fake websites.

Check the URL:

Fake websites often have misspelled or slightly altered URLs compared to legitimate ones. Legitimate websites typically have secure connections (https://) and a consistent domain name.

Verify Contact Information:

Fake websites may lack clear contact information or have only an email address without additional details. Legitimate websites provide multiple ways to contact them, including a physical address, phone number, and customer support.

Reviewing the Website Design:

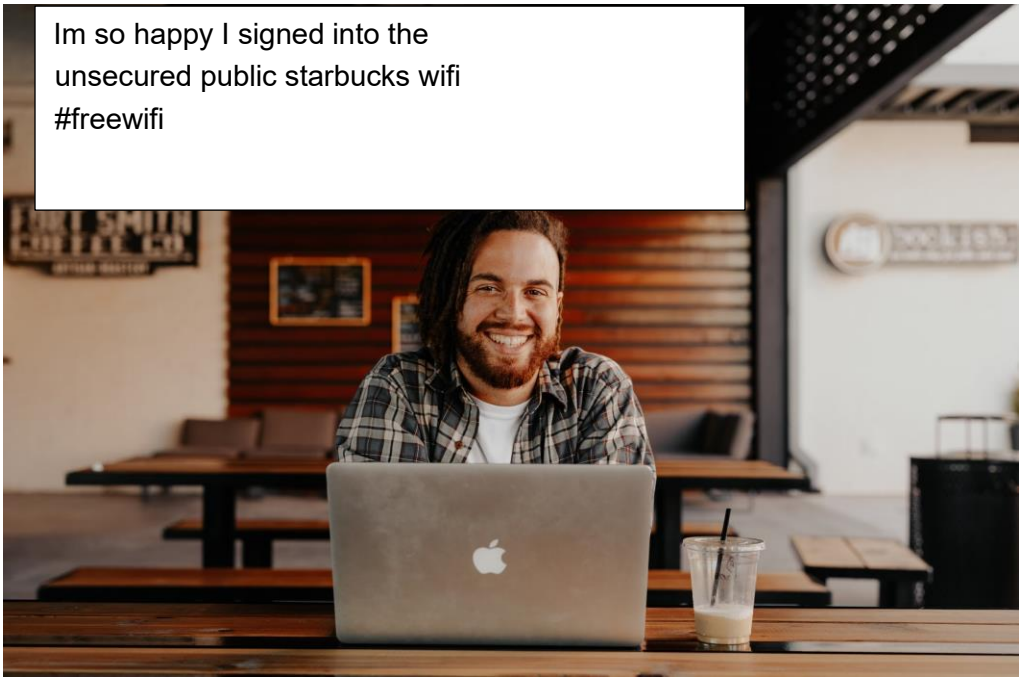
Fake websites may have poor design, low-quality graphics, and a general unprofessional appearance. Legitimate websites invest in professional design, have a consistent layout, and ensure a positive user experience.

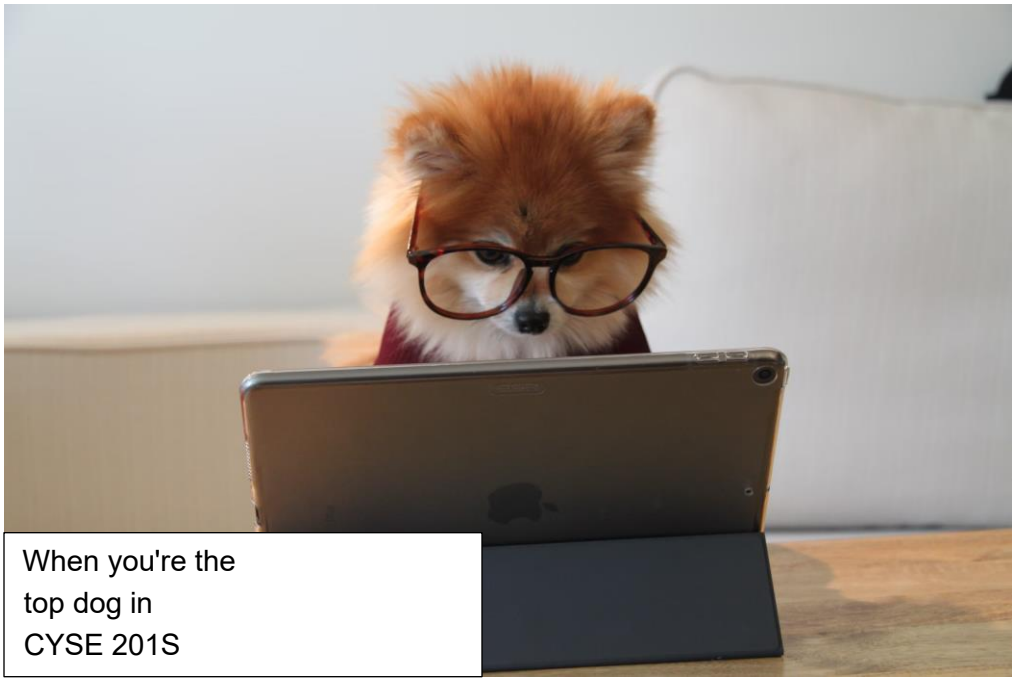
Check for Typos and Grammar:

Fake websites often contain numerous typos, grammatical errors, or awkward language.

Journal Entry #7

Question : Review the following ten photos through a cybersecurity human systems integration framework. Create a meme explaining what is going on in the individual's or individuals' mind(s).


Im so happy I signed into the
unsecured public starbucks wifi
#freewifi


When you're the
top dog in
CYSE 201S

When you're a cybersecurity guru but can't resist scrolling through Instagram

Journal Entry #8

Question: After watching the video, write a journal entry about how you think media influences our understanding about Cybersecurity.

Media plays a significant role in shaping public perception and understanding of cybersecurity. The portrayal of hacking and cybersecurity in movies, TV shows, and other forms of media can influence the way people perceive the field, its challenges, and the individuals involved. The video offers insights into how media representations of hacking and cybersecurity often blend reality with dramatization.

Sensationalism and Exaggeration: Media tends to sensationalize hacking activities, portraying them as fast-paced, intense, and capable of achieving almost magical feats. The video highlights instances where the depiction in media is exaggerated for dramatic effect. For example, the ease and speed with which hackers gain access, manipulate systems, or take control of physical objects are often exaggerated for entertainment purposes. In reality, such activities might require more time, planning, and sophistication.

Educational Value: Despite the dramatization, media can serve an educational purpose by introducing real-world concepts and terminology. The video points out instances where accurate terms like SQL injections, polymorphic code, and capture-the-flag competitions are mentioned in the context of fictional scenarios. This can contribute to raising awareness about cybersecurity practices and challenges, albeit in a dramatized form.

Impact on Public Perception: Media representations shape public perceptions of hackers and cybersecurity professionals. Characters like Elliot from Mr. Robot are portrayed as highly intelligent individuals capable of near-instantaneous hacks. While this may make for compelling storytelling, it can lead to unrealistic expectations about the capabilities of cybersecurity experts in the real world.

Influence on Security Practices: Media depictions of hacking can sometimes influence real-world security practices. For example, scenes involving social engineering or spear-phishing attacks in the video highlight tactics that attackers may use to exploit human vulnerabilities. This can serve as a reminder for individuals and organizations to remain vigilant and adopt security measures.

Balancing Entertainment and Accuracy: There is a delicate balance between creating an entertaining narrative and presenting accurate information. While media tends to take creative liberties for the sake of storytelling, it's essential for viewers to understand the line between fiction and reality. The text, through its analysis of various scenes, emphasizes the need to approach media representations of hacking with a critical eye.

In conclusion, media significantly influences our understanding of cybersecurity by shaping perceptions, introducing terminology, and providing glimpses into the world of hacking. While dramatization is inherent in entertainment, it is crucial for the audience to approach these portrayals with a discerning mindset and seek accurate information to comprehend the complexities of cybersecurity in the real world.

Journal Entry #9

Question: How did I 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 a 3 out of 9. This means I do not have SMD. The items in the scale are seem to be designed to assess various aspects related to social media use. I believe the access to technology and social media platforms, as well as the prevalence of digital culture, can differ significantly between regions and demographics, contributing to variations in social media use patterns. Also, factors like cultural attitudes towards technology, societal norms, and individual coping mechanisms can influence these patterns.

Journal Entry #10

Question: Read this and write a journal entry summarizing your response to the article on social cybersecurity.

The article I read into an insightful article on social cybersecurity, a burgeoning subdomain of national security with profound implications for contemporary warfare. The article illuminated the multifaceted nature of social cybersecurity, emphasizing its role in understanding and forecasting cyber-mediated changes in human behavior, societal dynamics, and political outcomes.

The notion that information warfare is evolving into an independent entity, rather than merely a component of hybrid warfare, struck me as a pivotal shift in the landscape of conflict. The article's focus on Russia's information blitzkrieg underscored the strategic impact of manipulating beliefs and values in the global arena, showcasing how information can be wielded as a potent weapon to weaken trust in institutions and sow discord across societies.

A key takeaway was the distinction between social cybersecurity and traditional cybersecurity. While the latter deals with the hacking of technology systems, the former involves the manipulation of humans through technology. The article's emphasis on the multidisciplinary nature of social cybersecurity, integrating fields from political science to social psychology, highlighted the complexity of this emerging domain.

The BEND model introduced in the article provided a framework for understanding forms of maneuver in social cybersecurity. From misdirection

and hashtag latching to opinion leader co-opting and the use of bots as force multipliers, the tactics outlined demonstrated the diverse arsenal available to actors in the social-cyber domain.

In reflecting on this article, I am struck by the evolving nature of warfare and the profound impact of information in shaping the outcomes of conflicts. The integration of technology with social and psychological aspects adds layers of complexity, demanding a nuanced and interdisciplinary approach. As I consider the implications of social cybersecurity on national security, I am reminded of the dynamic and ever-changing nature of the digital battlefield, urging continuous adaptation and vigilance in the face of emerging threats.

Journal Entry #11

Question: 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.

The presentation on the role of a cybersecurity analyst inadvertently touches upon several social themes. The emphasis on the entry-level nature of the job and the willingness to work unconventional hours reflects societal norms and expectations regarding career paths and work-life balance. The mention of networking underscores the importance of social connections in career advancement, reinforcing the pervasive influence of interpersonal relationships in professional spheres. Additionally, the discussion on salaries in different cities highlights the socio-economic disparities that exist across various regions, impacting individuals' choices and opportunities based on their geographical locations. Overall, the presentation subtly shows how societal norms, professional networks, and economic factors intersect and influence the trajectory of careers in cybersecurity, revealing the interconnectedness between individual aspirations and broader social contexts.

Journal Entry #12

Question: describe how two different economics theories and two different social sciences theories relate to the letter.

In the context of GlassWasherParts.com's data breach notification, economic theories such as Supply and Demand and Game Theory offer valuable insights. The Supply and Demand theory is relevant to understanding potential economic impacts on the company; a decrease in customer trust (demand) might necessitate strategic adjustments in pricing or efforts to rebuild trust. Game Theory is applicable to analyzing the strategic interactions between GlassWasherParts.com, customers, credit card companies, and law enforcement, highlighting the decision-making process influenced by the potential reactions of various stakeholders.

On the social sciences side, Social Identity Theory explains how the breach notification can influence customers' perception of their social identity as consumers. The disclosure of a data breach may alter customers' social identity, and the company's response plays a crucial role in shaping whether customers maintain a positive social identity. Additionally, Conflict Theory, from a sociological perspective, helps analyze potential conflicts arising from the breach, such as conflicts between GlassWasherParts.com and affected customers or conflicts between customers and credit card companies. Understanding these theories provides a comprehensive lens for assessing both economic and social implications in the aftermath of a data breach.

Journal Entry #13

Question: 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.

The article provides a comprehensive analysis of bug bounty programs in cybersecurity, with a primary focus on HackerOne's dataset from August 2014 to January 2020. The literature review offers a detailed overview of bug bounty dynamics, emphasizing the impact of factors such as program scope, bug severity, and the growing popularity of such programs. The study

addresses gaps in previous research, boasting a robust dataset that includes both public and private programs, and introduces an instrumental variable strategy for causality establishment.

The methodology is well-structured, employing OLS regression models, 2SLS regressions, and fixed effects regression to control for endogeneity and other biases. The use of a comprehensive dataset, encompassing various industries and program types, contributes to the external validity of the findings. The study introduces novel insights into the bug bounty market, including the calculation of the price elasticity of hackers, emphasizing the inelastic nature of hacker supply.

Key findings include the price inelasticity of hackers, indicating that monetary incentives are not the sole motivators for bug hunters. Bug bounties are found to be effective across companies of different sizes and prominence levels, democratizing access to IT talent, especially beneficial for smaller enterprises. The study also delves into industry effects, revealing variations in the number of vulnerability reports across different sectors, with financial and retail industries receiving fewer reports.

While acknowledging the impact of new programs on hacker competition, the study finds that their influence on the reports received by companies is marginal and statistically insignificant. Programs, over time, receive fewer valid reports, highlighting the need for continuous adaptation in bug bounty strategies. However, the article acknowledges that a significant portion of the variation in vulnerability reports remains unexplained, leaving room for future research.

In conclusion, the article makes a substantial contribution to bug bounty literature by addressing methodological limitations of prior studies and providing valuable insights into the bug bounty market dynamics. The findings have implications for bug bounty platforms, enterprises, and security researchers, emphasizing the need for ongoing research to enhance our understanding of this evolving cybersecurity landscape.

Journal Entry #14

Question: Review what the author says and write a paragraph describing the five most serious violations and why you think those offenses are serious.

The five most serious violations outlined in the text are streaming content through unofficial services, using torrent platforms for piracy, sharing copyrighted images without permission, engaging in cyberbullying and trolling, and recording VoIP calls without consent. These offenses are particularly serious due to their potential to cause significant harm to individuals, businesses, and the broader online community. Firstly, streaming through unofficial services not only violates copyright laws but also poses a threat to users' personal data security. Torrent services facilitate widespread piracy, directly impacting content creators and undermining the principles of intellectual property. Sharing copyrighted images without proper authorization infringes on the rights of creators and can lead to legal consequences. Cyberbullying and trolling contribute to a toxic online environment, causing emotional distress and, in extreme cases, leading to severe psychological consequences for the victims. Recording VoIP calls without consent violates privacy rights and can be exploited for malicious purposes. These offenses collectively highlight the importance of respecting legal boundaries, safeguarding privacy, and fostering a secure and ethical online space.

Journal Entry #15

Question: Write a journal entry describing what you think about the speaker’s pathway to his career.

This video is from a digital forensic investigator, and his career path was nothing short of intriguing. Starting as an accountant, he found his way into the world of digital forensics, a field at the crossroads of technology and investigation. What stood out was his genuine passion for the work, evident in his description of tracing digital footprints and solving intricate puzzles.

His journey reflects the dynamic nature of careers, showcasing how unexpected opportunities can lead to fulfilling paths. The talk highlighted the rapid evolution of technology, from floppy disks to dealing with one-terabyte machines. The case study he presented, involving a company facing government scrutiny, provided a real-world glimpse into the complexities of digital forensic investigations.

In retrospect, this video left me with a appreciation for diverse career trajectories and the importance of adaptability. It made me reflect on my own journey and the unforeseen possibilities that might shape my future career as a Naval Officer.