Journal 1 Prompt: "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."

I've been finding it extremely difficult to narrow down exactly what I want to do when I earn a computer science or cybersecurity degree. What I can do in the present is showcase my experience and knowledge I've equipped over the past few years, give an idea of what I want to focus on in the future and give an idea of where I want to end up after gaining seniority in the field after years of working.

I had the privilege of growing up during the peak industrial revolution of computer systems. The first game I ever played on a PC was Doom (from 1993) and I remember having a computer class in elementary school where the teacher cut a slot in a box to put over the keyboard for us to learn to type. Although I've had an interest in computer systems from a young age, I didn't start applying myself to learning about them until 2020 after I was discharged from the military. When I moved to Virginia Beach, I fell into a job opportunity of Data or Telecommunication Technician. I was fortunate enough to travel the country to work federal jobs where the FBI or Army wanted a complete data system upgrade from the communication closest to the user workstation.

As a telecom tech, I've been able to shrug shoulders with federal IT personnel like Electronic Technicians, Network Administrators, Cybersecurity Specialists. I was absolutely hooked to earn a degree in cybersecurity but now that I'm here, what now? The Workforce Framework for Cybersecurity (NICE Framework) gives a great breakdown of what different

cybersecurity personnel do in the field. After browsing what different subdivisions do in the cyber or IT field, I think I'm gravitating more towards the investigative side of the business. A few categories I'm interested in would be cyber investigations and digital forensics but I would also be very interested in cyber defense analysis and incident response. The categories that appeal the least to me would be the realm where IT specialists operate because I've met a few of them and they usually are given ten cents and are told to squeeze a dollar from it.

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

A scientific principle is a truth that is widely accepted by scientists. This is important because they can apply those certain principles as foundation for other studies. The principles of science relate to cybersecurity through a social science framework.

It is argued that the social sciences adhere to the same concepts as the natural sciences. To explain further, a few of the social sciences that can be scientifically applied to cybersecurity could be relativism, objectivity, parsimony, objectivity, skepticism, ethical neutrality, and determinism. A quick example of how these social sciences can be applied to cybersecurity could be exploring the thought of determinism when people chose to hack and commit cybercrime. In this example, the researcher ultimately is faced with a philosophical question of free will versus determinism (no free will).

Like how a social science framework can be applied to cybersecurity to drive research or obtain certain goals, societal systems and their principles can be related to cybersecurity as well. A few examples of detrimental societal systems that are related to cybersecurity could be educational, political, technological, criminal justice, critical infrastructure, healthcare, and

social systems. These important social systems relate to cybersecurity because they all rely on some degree of cybersecurity to operate and communicate with each other effectively.

The principles of science relate to cybersecurity because the same principles that adhere to natural sciences relate to social sciences. An example of how these sciences are relatable could be how a researcher develops a solution or scientific theory for a problem. This scientific method could be applied to organic chemistry or psychology to provoke research questions and provide solutions.

Journal 3 Prompt: "Visit PrivacyRights.org to see the types of publicly available information about data breaches. How might researchers use this information to study breaches?"

Researchers can use this information to study breaches by learning what was sought after, who aided the breach, how many people were affected and what we can do to combat these types of breaches. An easier way of explaining my thought process would be the 5 Ws: Who, what, when, where and why?

It's important to gather accurate information on a mass scale so researchers can study data breaches. Another example of this type of research could be how criminologists work with police to study the principles of sociology, psychology, economics, anthropology, and statistics. Why do researchers need accurate data? So they can formulate a plan to try to thwart the crime they're studying.

The 5 Ws of data breaches, or any crime in that sense, are extremely important to researchers trying to combat them. Who? One may ask who breached the data and who had so much data to be breached. What? What were the breachers searching for and how can we reinforce the security where this data is. When? When this breach happens or happened, can we

pull any patterns from how recent it happens? Where? Where is important because it gives researchers a good idea of what hackers are targeting for valuable information. Why? Why is extremely important because it gives us an idea of what kind of events could come since the data was leaked.

While some of the 5 Ws may be more important than the others when it comes to data breaches, they're all extremely important details that can lead to further questions researchers may have. Questions like: How much physical or emotional damage can be done with this sensitive information from this data breach? Where do we have to secure our systems more so we can protect our information better? Like criminologists, data breach investigators having a plethora of accurate information about a certain crime gives them the ability to recognize crime patterns, actively defend against other similar crimes, and actively secure systems that are designed similarly.

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

"Abraham Maslow's Hierarchy of Needs suggests that all humans have needs that exist on a hierarchy. The theory suggests that as our lower-level needs are met, we begin to focus on our upper-level needs" (Module 4 Slides). Maslow's Hierarchy of Needs breaks down into three main levels: Basic needs, Psychological needs, and Self-fulfillment needs.

To dive deeper into basic needs and how my digital experiences relate to them, one must understand that psychological needs (like warmth, water, food and rest) and safety needs (like

security and safety) are basic needs everyone strives to fulfill. I use digital technology every and/or all day to fulfill my basic needs. A few examples could be using a laptop to look up any information I need or using a phone to order food and/or call someone. Also, I fulfill my basic need of security and safety by having a phone on me all day (incase there is an emergency and I need to contact emergency services.

I also use digital technology daily to help fulfill my psychological needs. Not only can I use my cellphone to call emergency services and order the delivery of anything I need to my doorstep, but I can also use digital technology to instantly call or message anyone within seconds. Because I'm a human, I constantly feel the urge to satisfy my belongingness, love, and esteem needs. An example of how I long to fulfill these psychological needs would be how I can instantly send a message to a group chat that my mother and sister are in or I can call them at any moment I want.

It makes sense when someone applies the rules of Maslow's Hierarchy of Needs because some of my most challenging needs to fulfill are self fulfillment needs. This includes achieving one's full potential which could include creativeness or however that individual fulfills theirs. In my life, my self fulfillment needs are met by using digital technology to play music while I try my hardest to enjoy an activity like jogging, painting and skateboarding.

Journal 5 Prompt: "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."

4 types of psychological theories of cyber offending can consist of psychodynamic, cognitive, behavioral and personality theories. Psychodynamic theories suggest that early experiences in life influence behavior. Cognitive theories focus on the way individuals think and process information. Behavioral theories suggest behaviors are learned and personality theories explore how individuals' personal psychological traits contribute to behavior.

Individual motive depends on individuals and crimes. I would rank the first article a five out of seven. Five sounds accurate because the person who stole 700 million users' data from LinkedIn tried to say he did it for entertainment, but we all know he was trying to sell it. What doesn't make sense to me is why he would try to come off saying it was for entertainment. I would rank the second article a one out of seven. It is a fact that politics pushes some people to the edge and in this case, politics pushed "hacktivists" and "leaktivists" to use hacking in order to spread their ideology or try to make a certain group of people look bad. The third article deserves a one out of seven for making sense. Emotions from relationships push people to crime because of feelings of jealousy, depression and loneliness.

The fourth article deserves a three out of seven. The first thing parents should do if they let their children use high tech cell phones that are connected to the internet is set every parental advisory or setting they can to ensure their children are safe. Also, monitoring their children's internet use is extremely important. The fifth article gets a two from me. In this day and age of people doing crazy things for likes and followers, or digital recognition, it is very common for people to pull a wild stunt to attract internet traffic to their content. Also, the more internet traffic one can pull, the more potential money they can make from a side hustle like selling t-shirts or coffee mugs. The sixth article has a ranking of one out of seven as well. If there is anything someone is doing cybercrime for, it's cold hard cash. The seventh article is a one out of seven as

well. What is interesting about this article is that they dive into how complex a cybercriminals brain can be. It makes the most sense that most cybercriminals are feeling a mixture of emotions, monetary greed, and complex psychological traits.

Journal 6 Prompt: "Can you spot three fake websites and compare the three fake websites to three real websites, plus showcase what makes the fake websites fake? "

Why would someone create a fake website? One of the main reasons why someone would create a fake website is to phish information from someone else. Although it was hard to find fake websites when I looked for them, I did find an interesting article written by Tomas Meskauskas from PCrisk.com showcasing different types of Amazon pop-ups someone may be confronted with while surfing the internet. This article highlights popular current Amazon scams but it's common for scammers and cybercriminals to spoof other popular companies as well.

These scams would be considered fake websites because Amazon definitely didn't give the creator of the website permission to use their logo and name to draw victims in. Because every scam pop-up isn't the same, scammers are able to trick victims with this Amazon example, fake error messages, fake system warnings, pop-up errors and fake computer virus scans. One common thing all these scam pop-ups have is the creation of urgency or pressure to participate or one would lose the chance to win a free Iphone or one will have to now get their computer fixed.

There are different levels of damage that can be done when a victim takes the bait from one of these fake websites. A few examples of the damage that can be done could be simple personal information gathering (name, address, phone number, email address), fraudulent

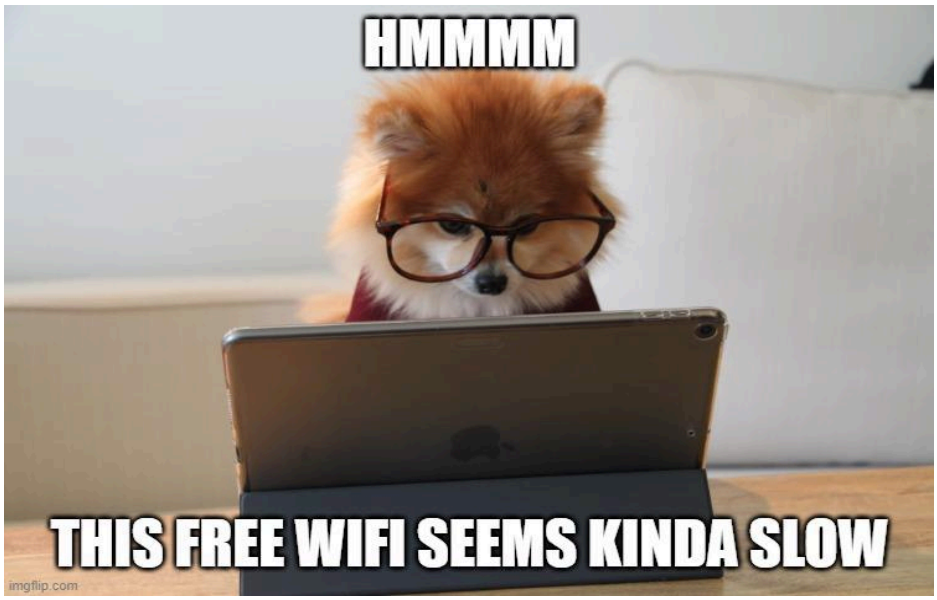
information gathering (credit card numbers, social security numbers) and victims sending money to scammers to “fix their computer” or “payoff debt”.

The most important way someone can protect themselves from participating and giving information to these scam websites and pop-ups would be being knowledgeable and aware of how these scams work, what they commonly look like and how to report them. A few red flags every internet user should look out for are typos on a website (especially a big website like Amazon), a sense of urgency, an odd looking URL and the need to question if something is too good to be true.

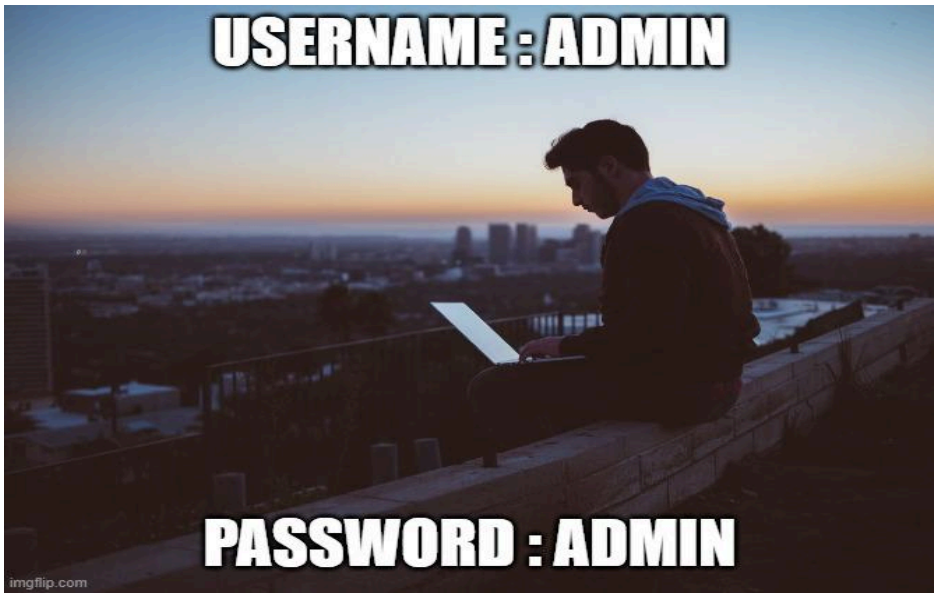
Journal 7 Prompt: “Review the following ten photos through a human-centered cybersecurity framework. Create a meme for your favorite three, explaining what is going on in the individual’s or individuals’ mind(s).”

Human centered cybersecurity is an approach to cybersecurity that recognizes that humans are a critical part of security. It also focuses on adapting to human behavior, psychology and interaction.

Most of us have been part of the classic cybersecurity meeting where the IT department tries to educate the rest of the employees about common phishing scams that attempt to rope victims in. The different ways scammers will try to steal information from unsuspecting people could be romance scams, congratulations scams,



unclaimed money scams and virus scams. The human centered solution to phishing scams would be to send mass emails to employees warning or educating them on what to look out for while browsing the internet on work computers. All it takes is for someone to accidentally download malware or accidentally give important information about the business away (OPSEC) to shut the business down for days, weeks or months. A tactic some hackers use to steal information like usernames and passwords are called man in the middle attacks or MITM. The way bad actors are able to do this is by mimicking a company's real wifi and relaying or possibly altering two parties that think they are directly communicating with each other. The human centered way to defend against this type of cyberattack would be having knowledge of how common it is and having a zero trust factor. A few common ways to know you're being intercepted is an abnormally slow connection or if you were mysteriously logged out of something you were logged into before connecting. Some more advanced ways of detecting this would be authentication or tamper detection.



Strong passwords are extremely important to cybersecurity. Some could argue that a network is only as strong as its weakest password. The human centered way of strengthening the passwords of users in a network you're responsible for could be creating and delivering everyone's passwords for them. This will also take out the possibility of someone forgetting their password and the extra work that would create.

Journal 8 Prompt: "After watching the video, write a journal entry about how you think the media influences our understanding about cybersecurity. Has this understanding changed over time? What is different in the older pieces of media vs more current media? "

Like cybersecurity and hacking, the stereotypes given to hackers have evolved over the years. Many may claim that the stereotype of yesterday would label a hacker as a socially awkward person sitting in a dimly lit room with a hood on typing a thousand miles per hour while a hundred screens pop up on their computer screen. The films these hackers rated gave solid proof to how hacker stereotypes evolved.

What I realized about hacker stereotypes is that there are levels and they are based on how wrong or right the director or editor was about a certain cybersecurity topic. An example of being kind of right would be like how The X-Files (1997) almost covered the topic of hacking government systems the correct way then proceeded to reference ARPANET which was what the internet came from.

Because cybersecurity is a subculture in itself, it's hard to depict it from face value now and it was since the birth of technology. A film that dissected the complexity of a hacker in a more realistic way could be Mr.Robot (2015). Like how a criminologist takes different social sciences into account when analyzing a crime or a criminal, hackers prove to be complex too over and over again. Some hack for monetary gain, some hack for the rush of it, and some hack because they're peer pressured into it.

The stereotype of a hacker has evolved since the inception of it and the best way to describe it is that it used to be cringy and misunderstood but with the evolution of technology, the internet, and the social sciences, "Hollywood" is seeming to catch up with what a hacker truly is: complex.

Journal 9 Prompt: "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? "

In the video "How Cybercriminals Can Use Your Social Media Activity Against You", uploaded by Trend Micro, Rick Fergesun had a few great observations and pointers about how one can approach using social media responsibly. Rick, the Vice President of security research at

Trend Micro, explains how accepting any connections (like messages or friend requests) on social media can be extremely dangerous. He supported his claim by showing the viewer how cybercriminals try to socially engineer people by posing as someone else to hopefully extract data from them. This can be achieved by gaining someone's trust with a fake friendship or tricking them into a romance scam.

He also mentioned that these methods of social engineering are “classic” and “can be done by anyone” which implies that it is quite easy to pull off and is well known. While Rick was showcasing an “attacker’s dream”, Dave, he talked about how Dave loves showing off extremely personal information about his life to hundreds of millions of people. This video was eye opening because Rick flawlessly highlights how free data is gathered and weaponized by a bad actor and this process is also called “reconnaissance” for a target. An example of an organization’s employees falling victim to a social engineering attack could be when Google and Facebook’s employees were spear phished for $100 million dollars between 2013 and 2015 by Evaldas Rimasauskas. One could argue that social media played a critical role in being able to contact such important employees of the tech giants.

If I completed the Social Media Disorder Scale 10 years ago when I was 18, I would’ve scored much higher than now. In 2014, social media like Facebook, Snapchat, Instagram and LinkedIn were booming like never before because of all the advances with smartphones and the internet. In my adolescent teens, I was completely addicted to social media, didn’t know how to use it safely and had absolutely no business putting all my personal information on it.

Now that I’ve matured, I understand that it’s not important for me to list all of my family members, friends, where I work, my birthday, and how old I am to the rest of the world. These days, I only use Facebook to keep in touch with family and job websites like LinkedIn or Indeed

for employment opportunities. I would say that I would score pretty well on the SMD Scale now because I'm well aware of the importance of my personally identifiable information.

Journal 10-2 Prompt: "Read this and write a journal entry summarizing your response to the article on social cybersecurity"

The journal "Social Cybersecurity - An Emerging National Security Requirement" by Lt. Col. David M. Beskow and Kathleen M. Carley highlights how social and network manipulation and misinformation can decentralize a nation. The main theme of this journal would be how technology advancement and anonymity have taken away the requirement for physical proximity to influence society and how the DOD and civilians need to be aware of the emerging information war.

One of the most interesting things I learned from this journal is how Beskow and Carley explained the different "forms of maneuver" when it comes to the social cyber domain. The BEND Model of Describing Social Cybersecurity Forms of Maneuver is broken down into knowledge and social network manipulation. While the B (build, bridge, boost) and E (engage, explain, excite) letters of BEND cover positive manipulation of knowledge and social network manipulation, the N (nuke, narrow, neglect) and D (dismiss, distort, dismay) letters cover the negative side.

Some methods of information maneuvering that were showcased would be misdirection, hashtag latching, smokescreening and thread jacking. Some examples of network maneuvering would be opinion leader co-opting and community bridging. These methods are used to spread misinformation which could change public opinion or corrupt societal ethics. One of the most

interesting things that I learned from this journal is how bots are used as force multipliers that can change public opinion due to “trolling” or public opinion manipulation. Social cybersecurity requires a multidisciplinary approach included with relevant policy and is a required discipline for the foreseeable future.

Journal 11-2 Prompt: “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 for identifying vulnerabilities in a company’s cyber infrastructure. To identify the vulnerabilities, ethical hackers are invited to try explore 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 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.”

Economic policy plays an important role in shaping the landscape of cybersecurity, like in the form of bug bounties, ethical hacking, and overall security advancements. By setting legal frameworks and incentivizing certain findings, economic policies can significantly influence how vulnerabilities can be identified and mitigated

Bug bounty programs, where individuals are rewarded for reporting security flaws, thrive under policies that recognize and protect the legal rights of ethical hackers. Policies that offer tax incentives for companies that invest in such programs can increase participation from businesses, making these programs more popular. On the other end of the spectrum, fearing legal repercussions of reporting vulnerabilities creates a gray area for penetration testers. The right

economic policies can create a more open, cooperative environment between businesses and ethical hackers, fostering a culture of security. Economic policies that support research and development in cybersecurity can lead to significant progress in the field. Government grants, subsidies, and tax breaks for cybersecurity initiatives can accelerate protection, making advanced security technologies more accessible and affordable. This, in turn, enhances the overall cybersecurity posture of not just individual organizations but also national infrastructure and global networks.

Policies promoting education and training in cybersecurity can expand the pool of skilled professionals, including ethical hackers and penetration testers. Investing in cybersecurity education equips more individuals with the skills needed to identify and address vulnerabilities, contributing to a more robust cybersecurity ecosystem. Economic policy is a crucial part of cybersecurity progress. Through supportive legal frameworks, financial incentives, and investments in education and research, policies can significantly enhance the effectiveness of bug bounties, empower ethical hackers, and create a more secure digital world.

Journal 12 Prompt: "Andriy 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."

Andriy explains in this article that using unofficial streaming services, torrent services, copyrighted images, and other people's internet networks may be things people do on the internet without realizing they are illegal. Sharing passwords/addresses/photos of others, bullying, and trolling, recording a VoIP call without consent, faking your identity online, collecting

information about children, extracting audio from YouTube, and searching for illegal things are also other offenses that are commonly committed. Of these eleven offenses, I believe that sharing passwords/addresses/photos of others, collecting information about children, and using other people's internet networks are more serious than media piracy. Using unofficial streaming services, downloading torrents, using copyrighted material, etc. has always been a hotplate for debate. The debate happens when people try to use someone's media for personal monetary gain without giving a portion of it to the creator. Modern-day copyright laws revolve around the "fair use" allowance under the Copyright Act 1976. Fair use means that people can legally use media for criticism, comment, news reporting, teaching, scholarship, education, and research. Sharing passwords, addresses, and photos of others is dangerous because it puts people at risk of identity theft, injury, etc. Collecting information on children under the age of 13 should stay illegal in my opinion, even if the child lied about their age to gain access to the site. Many would agree that the adult would be taking advantage of that child and could potentially be putting them in danger by collecting information on them without their parent's consent. Using other people's internet networks should stay illegal because bad actors can hijack someone's network to commit crimes and hide their real location. This puts the real network owner at risk of investigation because when the crime is being investigated, they will be targeted by law enforcement for investigation instead of the real threat.