

Cybersecurity Journal Entries

1. Watch [this video](#) and write a paragraph about how Ann's behavior is related to the need for cybersecurity. In addition, pay attention to the way that technological changes increased cybersecurity risks. By watching the video you will see that cybersecurity requires an interaction between human behavior and technology.

Ann's behavior is deeply related to the need for cybersecurity. Ann fell for the phishing attack and ended up giving up her credentials to the hacker. The hacker knew that she shopped at shoppingcart.com. The hacker then manipulated Ann by sending a phishing link fronting as a free gift voucher. This problem strives deeper than this one scenario. Every day, a plethora of device users are tempted by these fake emails and hacks. The only real way to combat them is cybersecurity. Other than the actual technical need for cybersecurity there is also an informational need. To prevent social engineering attacks and manipulation hacks, like Ann's situation, users have to know the safety concepts of cybersecurity.

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

There are a few categories that caught my attention when looking at the framework. Protect and Defend, Investigate, and Analyze all caught my attention. I would like to see myself Protecting the future company I work at from potential cyberattacks. Analyzing threats is also something I see myself doing. I want to be able to learn more about the different types of attacks and future learn how to combat new hacks. If in the scenario where I do not go the route of the first two then I see myself focusing on cyber investigation. I have always liked investigating and it seems interesting to do so online. Securely Provision appealed to me the least. I never had a real desire for software engineering and Securely Provision seemed to deal with scenarios including it so it didn't seem as interesting as the others.

- 3. I included a link to a video and asked you to explain how the insight from the former criminal might be used in cybersecurity studies. It turns out that I linked to the wrong video. I meant to link it to this video:**
<https://www.youtube.com/watch?v=0UuHn27dFpE>.

The former cybercriminal gave a lot of information about the ins and out of cybercrime, specifically on the deep and dark web. I think if one were to use what he said in the video, they would research cybercrime in both the deep and dark web. He said that the deep web is 400x bigger than the clear net. If we see so many cybercrimes happen on the clear net imagine the sheer possibility that could be happening in the deep and dark web. The former cybercriminal gave a lot of examples of the crimes that happen on the dark web. I think further research on these cybercrimes on the dark web would be beneficial to many. Research may help us stop drug trafficking, human trafficking, child pornography, stolen credentials, etc. We don't see this as often in the clear net. Most likely happens more on the dark web.

- 4. Is it ethical to study people in cyberspace when they don't they are being studied?**

I am on the edge about this question. Though I see it as strange to study people in cyberspace, I do not see it as unethical. In my opinion, I view cyberspace as the same as the physical world. Let me explain. In the world we live in, we have private areas as well as public areas. Parks, city streets, restaurants, etc. These are what we say are public areas which is also a space for ethical observational studies without the possible consent of the subjects. But we also have private areas in the physical world such as our homes, bathrooms, cars, etc. In these areas, we are not allowed to be studied, ethically, without our consent. This is how I see research in cyberspace. We have "public" areas in cyberspace where nonconsensual observational research is ethical. For example, Instagram comment sections, web forums, youtube comment sections, etc are what I believe to be some of the public areas in cyberspace. Like the physical world, we also have our private areas in cyberspace. Areas like our personal email, could files, personal account information, etc. These are areas that I think nonconsensual research would be unethical. My position is half and half. Depends on the situation and area where the research is taking place.

5. 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.

Motives for cyber offending depend on individuals and crimes. A link to an example of each motive is included.

- Entertainment
- Political
- Revenge
- Boredom
- Recognition
- For money
- Multiple reasons

- 1) Money makes the most sense when it comes to a possible motive for cybercrime. Most of the cybercrime I hear of deals with the topic of money. Either the cybercriminal taking the money for themselves or hacking for a paycheck from a third-party source.
- 2) Politics comes behind money in making the most sense. With countries, all around the world, becoming more technologically advanced we find that cybercrime between them is on the rise. For example, let's take a look at the Russian-United States election conflict. In past elections, the FBI has been looking into possible Cyber Russian influence in our presidential elections. They actually did find that the Russian was tampering with our vote server systems. Combat between countries has moved from physical to cyberspace. Countries gain information without any casualties and it is easier than the traditional method of spying. Cybercrime politically makes sense.
- 3) Coming in third is revenge. This one is a very common type of cybercrime. Some examples are revenge porn, workers hacking after being laid off, cyberbullying, etc. Many people want to enact revenge on someone but not physically hurt them. So to get their revenge they go to the internet.

- 4) Recognition is next. Moving away from cybercrime, let's take a look at regular crime. Every decade or so we have that one criminal that strives to be the biggest criminal known to man and be the best at it. The same thing applies in cyberspace, it's just that we see it more often. Some hackers want to be known for being the best, most adventurous, most brave, etc. It makes sense as a motive but compared to the first three, it just doesn't seem that logical.
- 5) Entertainment and boredom are on the same number. These both are somewhat the same motive. It makes sense that cybercriminals are bored and want entertainment from hacking but the fact that there are so many other ways to be entertained online just doesn't make that much sense to me. Though as we said in class black and gray hat hackers are linked to Machiavellianism and sociopathological mindsets which makes sense for them to hurt people online. Video games, ethical hacking, capture the flag events. These are alternatives to cybercrime.
- 6) Finally is multiple reasons. When it comes to cybercrime we want to be able to look beyond just the crime and look for a motive. When a cybercriminal has more than one and a mixture of the ones stated above is when it gets confusing. How are you supposed to find the sole motive when a cybercriminal shows evidence of multiple.

6. The specific experiences of cybersecurity professionals would also vary across work roles. In this [video](#), Sandra describes seven reasons why individuals should consider a cybersecurity career. Pay particular attention to the psychological fulfillment she describes from the job and the importance of psychology in cybersecurity careers. Based on what Sandra says, which factors do you find most interesting for those seeking cybersecurity careers.

After watching the video I found there to be two main factors that made my interest in a cyber career heightened. The first topic that interested me the most was the money aspect of the career. With cyber careers having very competitive salary amounts, workers tend to be paid well as Sandra said in her video. She said 65k was a common salary for someone starting off. For a salary right out of college 65k is pretty decent and there's a chance I could be getting more. The salary aspect of a cyber career is just too good to not pursue. The second fact is the aspect of never being bored and always learning. As Sandra said, cybersecurity is always changing and there are always opportunities to learn different areas of cyber and even learn the changes of your current position. It's exciting to think that if I obtain a career in cyber security that I would most likely never be bored. The position would never get stale. I can't see myself doing the same thing every day for the rest of my life. Change excites me.

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

- <https://unsplash.com/photos/mfB1B1s4sMc>
- <https://unsplash.com/photos/gySMAocSdqs>
- https://unsplash.com/photos/ICTKevnXx_8
- <https://unsplash.com/photos/Z3ownETsdNQ>
- <https://unsplash.com/photos/5QgIuuBxKwM>
- <https://unsplash.com/photos/R6dSBkz32B8>
- <https://unsplash.com/photos/BXiLSwwwvqrY>
- https://commons.wikimedia.org/wiki/File:Computer_user_icon.svg
- https://commons.wikimedia.org/wiki/File:Summer_school_GLAM_giorno_1_1.jpg
- [https://commons.wikimedia.org/wiki/File:CellPhone_\(16491636068\).jpg](https://commons.wikimedia.org/wiki/File:CellPhone_(16491636068).jpg)

Explain how your meme relates to Human Systems Integration.



When your company hires a cybersecurity firm as well as firewall software to defend from hackers

This meme relates to human systems integration because when looking at the capabilities of human cyber professionals we see the limitations to the actual work they can do. Hiring a firm for example is a plus, but without literal software, they are merely people on your network.

Integrating this system so the human factors are not limited is the goal. Thus why the lady in the picture is so happy.

8.) Your free-write for this week is to watch this video and pay attention to the way that movies distort hackers. H [Acker Rates 12 Hacking Scenes In Movies And TV | How Real Is It? - YouTube](#). After watching the video, write a journal entry about how you think the media influences our understanding of cybersecurity.

I think that the media makes hacking more complicated and more entertaining than it really is. As Elazar said, the media may add sprinkles of realism to the movies and shows but it thinks to add that sense of entertainment value they have to make it look cooler than it really is. I think this can be a good thing and a bad thing. The way I got into cybersecurity was through movies and video games. They always looked cool and seemed like something fun to do. But the negative is that it could scare a lot of people away because they think that it is maybe too hard and maybe a little intimidating. I also think that it makes the hacking look scarier. Though hacking may be very scary, the level of attacks they show in the media, I don't think, is as bad as attacks truly are. I think that the hacks they show in the media are the worst of the worst. People getting their cameras hacked and all those extreme types of attacks. Though these happen, I do not believe that it is as easy to do as portrayed in the media.

9.) Journal. Watch [this video](#) about a 12-year-old cyber security expert. Pay attention to how he has embedded himself into the cybersecurity culture. Also, pay attention to how the ideas of knowledge, technology, and secrecy related to his expertise. Write a journal entry about your thoughts related to the video.

It's very impressive that someone of that age can even comprehend that type of information. Mr. Hacking ninja made a good point that if a twelve-year-old has the capability to hack, think of how easy it is for an adult to learn hacking for harm. As I was watching I was recollecting back to our discussion about the studies of hackers and youth. I was thinking about some of the characteristics youth hackers have. I think the stable household made him an ethical hacker. When we discussed in class we learned that adolescents with possible resentment to their parents and peers are most likely to be hackers. We also learned that accessibility played a big part in hackers in youth. I think Rueben had easy access to internet technology, but I believe that the reason he has a good home life separated him from being a black hat hacker. But in the end, It goes to show that anyone can learn how to hack. No matter age or who you are.

10.) Watch [this video](#) and relate it to class lectures about subcultures.

First off I want to say, I found it hilarious that this video is the topic of one of our journal entries. After talking about criminal subcultures in class I can now see how this video and its scammer subculture relate. In the video, we hear about the various scams the rappers talk about and what they do with the wealth gained from the scam. This relates to the criminal subculture because of how the artists are rapping about how they work together to scam. In the song, they all talk about scamming basically putting them all in the subculture of scamming. And it makes sense because in the song they also talk about communicating with other scammers vs Internet, online payment services, etc to scam.

11.)•Watch this video. As you watch [the 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.

Early in the video, Nicole gives a general description of the task needed to do by the cybersecurity analyst. Especially for newcomers, dealing with the social aspect of cybersecurity is going to be a big part of the job. She relates newcomer cyber analysts as “cyber security help desks”. As Nicole said in the video you are going to possibly be responding to phishing emails that deal with the social engineering part of cyber and also offer cyber safety guidance and training to your fellow coworkers. What I took from the video is that in the beginning as a cyber analyst, you are going to be dealing a lot with the possible social engineering attacks your company deals with and ensuring that your company and coworkers stay away from such attacks.

12.) Complete the Social Media Disorder scale. How did you score? What do you think about the items on the scale? Why do you think that different patterns are found across the world?

After I took the scale test. I found that I only said yes to two of the questions. I think that these questions, in a sense, relate to those found when diagnosing a possible substance addiction. With my mom being a SARP counselor, I have gotten to learn a thing or two about addiction. The questions on this scale are very similar. I think all of the questions on the scale are valid points to diagnose a social media disorder. On the topic of different patterns across the world, I think it depends on the stage of the country as well as the government's feelings on social media. For example, some countries have little to no access to internet technology while some countries' whole population is on social media. These reasons are going to make the number of users vary

across the globe. Especially with countries that censor social media like North Korea, China, Iran, etc. This will also skew the patterns found across the globe.

13.)• [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.

While some of these things on his list are not illegal, I will say that all of them are frowned upon. I think the most serious violation on the list is bullying and trolling. I put this one as number one because this violation is the one, I believe, that can cause someone to hurt themselves or hurt others. Though face-to-face bullying still exists, most of the time, recently, bullying takes place on the internet. This can lead to suicide, potential motives for physical crimes, and degradation of mental health. The second serious violation I said would be collecting information about children. This is just downright weird and wrong. We have a specific act protecting children from this and without consent kids' data shouldn't be taken nor used. The third most serious is going to be faking your identity. When it comes to faking identities online, most of the time it is used for fraudulent purposes. This one is number three because it's technically not illegal to make an account being someone you're not. It's when it is used for fraud when it gets serious. The 4th serious violation is going to be using copyrighted images. Though you can pretty much use any image on the internet with proper permission and citation, this one is on my list because I think people use copyrighted images for fraudulent purposes as well. When we look at fake social media accounts, most of the time, the images of the people are taken from other people on the internet. 1 the person is using an image without consent and proper permission and 2 they have the possibility to use it for fraud. Last but not least on my list. Unofficial streaming. This is definitely a big problem when it comes to cyber violations. It is illegal to watch videos, sports, etc without the proper rights and permission. It's on my list because it is illegal, but low on the list due to the fact that we rarely see people being prosecuted for it. It's common to see but an uncommon thing to see punished. Though I do not condone piracy, I am merely saying that I found that it is an offense that is usually not punished that often.

14.)Read ODU's [electronic communications policy](#). Write a paragraph describing how it relates to cybersecurity.

When I skimmed through the policy the code that caught my attention was 09.1.0 Acceptable Use Standard. In summary, this code discusses what a user can do and access on ODU owned devices and ODU networks. I think this regulates people doing unlawful things on the internet and promotes that such devices and networks are used for strictly school purposes. Other than preventing school users to commit cybercrimes this code and policy help to prevent our users from being attacked by possible cyber attacks. With less exposure to sketchy websites and websites not allowed by ODU networks(via this policy and the network filters), there's a less likely chance for there to be cybersecurity risk. Other than this policy, there are multiple procedures to protect student information such as FERPA. The whole point of cybersecurity is protecting students, people, and their data. So this act definitely has a lot to do with cybersecurity and the protection of our data and internet safety.

15.)What does AI have to do with cybersecurity

Though humans are always going to be needed when it comes to cybersecurity, we are seeing that AI is increasing the protection we are able to have when it comes to cyber threats. When AI is applied to cyber security, multiple sectors are able to be covered more efficiently than humans can do. For example, In the sector of identifying threats and identifying vulnerabilities, we are seeing that AI is able to find more threats and vulnerabilities than our traditional way of finding them. When it comes to identifying threats, AI is able to find more threats in a less amount of time compared to the traditional way of signature-based techniques(Segal). Though this may be beneficial it also comes with the downside of yielding false positives. AI in certain sectors is proving to be very beneficial but must coincide with our traditional ways to yield the best results.

Segal, Eddie. "The Impact of AI on Cybersecurity: IEEE Computer Society." *IEEE Computer Society The Impact of AI on Cybersecurity Comments*,
<https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity>.

16.)How do the social sciences inform our understanding about the interconnection between AI and cyber?

The social sciences are very important when it comes to the interconnection of AI and cyber. When we use a social science lens when looking at cybersecurity we look at the human factors that play into either cybercrime or cyber victimization. Using this found knowledge we are able to help create the bridge between AI, Cybersecurity, as well as the social sciences. An example of how we are able to do this is by using machine learning and artificial intelligence to help us identify the ways people are interacting with the internet to either offend online or become victims online. Though this may not make our traditional way obsolete, professionals are able to cover more ground in a less amount of time. In conclusion, we use our social

sciences to create AI to help us understand human vulnerabilities, thus helping us defend ourselves online via cyber.

17.)A [CNN host](#) recently said he'd rather give his kids Jack Daniels and weed than Jack Daniels. What do you think about this statement?

Though I do not condone the use of drugs and alcohol in kids that are under the age of legal use, I do agree with the host's statement to a certain extent. While I do believe that the host meant this statement figuratively and not literally, his statement does carry a lot of weight when it comes to social media. With almost half of the world's population being on social media, studies have shown that the use of social media has actually become an addiction. With this being said, I can see where the host is coming from. On the other hand, social media has become a ground to share, interact, and communicate with everyone around the world. I think what the host was saying by this comment is that he thinks social media has more negative effects than positive. Was his comment unprofessional? Yes. But do you really think he is going to give his kid weed and jack?

18.)Why do you think victims don't report cyber victimization?

There are a lot of reasons that victims do not report cyber victimization. These reasons can range anywhere from victims not knowing how to report it and even victims being too embarrassed to even report it. I actually have a story about a victim being too embarrassed to report it. This is a story about my little brother. With him being young and not knowing any better, he decided to click on an email saying that he won free "vbucks".(an in-game currency in the video game Fortnite). After he clicked on it he ended up getting porn ads in the calendar and notes app on his phone. With him being so young he was scared and ultimately embarrassed to tell either me or my dad. With this being said, it wasn't until a couple of weeks after the hack that he decided to tell me. When I got his phone I ended up clearing everything up on his phone and had to reassure him that he wasn't in trouble and that it wasn't his fault. I had to keep telling him that if he ever suspected he got hacked to not be afraid to tell me. Though he and I got everything cleared up, it just goes to show how victims sometimes are too afraid or even embarrassed to even tell someone that they became a victim online.