For my article review, I chose an article from the "International Journal of Cybersecurity Intelligence & Cybercrime." The article is entitled; "Level of Engagement with Social Networking Services and Fear of Online Victimization: The Role of Online Victimization Experience." *(Park, Y., & Vieraitis, L. M. (2021). Level of engagement with social networking services and fear of online victimization: The role of online victimization experiences. International Journal of Cybersecurity Intelligence and Cybercrime, 4(2), 38-52. https://www.doi.org/10.52306/04020421TERZ5728)*

Engagement and Victimization

Yeonjae Park and Lynne M. seek to determine how the level of engagement with SNS (Social Networking Services) relates to the fear of online victimization. Their findings show the diverse types of effects the level of social media engagement has on fear, including indirect and direct relationships. Their findings seek to support the hypothesis that "greater SNS usage increases the risk of online victimization, leading to a greater fear of victimization on SNS." *(Park, Y., & Vieraitis, L. M. (2021).* These findings along with the ever-growing use of social media can help policymakers determine how to best help social network users stay safe in an online environment while also maintaining engagement.

Cyber victimization involves the risk of several cybercrimes, including malware, social engineering, cyberbullying, and identity theft to name a few. According to a study conducted by Brunton-Smith & Sturgis, 2011 and Gainey et al., 2011, several risk factors are associated with a heightened fear of crime. These types of fears include: "economic disadvantages, social roles & protection, neighborhood characteristics, and the amount of consumption of social media." *(Park, Y., & Vieraitis, L. M. (2021)* However, what sort of factors impact a heightened fear of cybercrime? Examples of this could be prior victimization, perceived risk, and cyberbullying.

A prior victimization of a cyber-attack has been found to cause social media avoidance, increased fear, and a feeling of reduced freedom in social networks. Perceived risk, for example, was found to positively affect the fear of online victimization in all types of victim-offender relationships. According to an investigation conducted by Randa (2013), prior cyberbullying increases fears of victimization on several online services among youth. All three of these examples support the hypothesis that "prior victimization impacts present fear of cyber victimization." *(Park, Y., & Vieraitis, L. M. (2021)*

Social Science Principles

An example of how the principle of social science is used in this article includes: determinism, skepticism, and relativism. Determinism is demonstrated by the prior event of victimization; this prior event now leads to the current heightened sense of fear around cyber-attacks. Skepticism in this issue can involve one's distrust of current cyber security standings, such as the promise of complete data security and transparency. Finally, relativism describes how all an individual's actions relate to a cyber security incident. For example, someone may have clicked on a "free" iPad pro link, which led them to a fake credential prompt, stealing their social media username and password, and hijacking their account. All these events are related, as the first choice of clicking that link interconnected all of them.

One of the research methods used by this article was finding different theories and describing how they are connected to cyber security. For example, the "*Routine Activities Theory"* is described. This theory states that, "postulated crime occurs when three elements converge- motivated offenders, suitable targets, and the absence of capable guardians." *(Park, Y., & Vieraitis, L. M. (2021)* Motivated offenders in cybercrime could be those seeking financial or personal gain. Suitable targets in the world of cybercrime involve those with poor security hygiene, those who engage in risk internet behavior, (ex. Clicking links, downloading unauthorized content, using outdated software). Capable guardians include proper antivirus software, cyber security knowledge, and consistent backups of files.

Another research method is analyzing data. This article utilizes a study conducted by the "Korean Institute of Criminology." This study administered surveys of 1,000 adolescents and who use one of four common social media sites. They are Facebook, Twitter, Kakao Story and Cyworld. The independent variables of this study were "Level of SNS engagement and Victimization experiences." The dependent variable of this study was, "Fear of Victimization on SNS." Finally, the control variables were gender, age, highest level of education and monthly average income. The averages for this study were thirty-two, with some college education and a ₩3,500,000 average monthly income ($2,636.55 USD).

The results of this study show that a higher level of social media engagement positively correlates with the fear of victimization. However, gender and income were negatively correlated with this fear. The level of engagement on SNS positively correlated with victimization experiences. According to the results of the study, the control variables on fear of victimization

on SNS presented as follows: " gender ($\beta = -1.82$, $p < .001$), age ($\beta = -.00$, $p > .05$), education level ($\beta = .42$, $p < .05$), and income ($\beta = -.48$, $p < .01$)." *(Yoon & Park, 2014).* This data analysis study concludes that the level of SNS engagement has a significant correlation with victimization.

Class Concepts

This article relates to a few of the concepts we have learned in class, they include multi-method research, cyberpsychology, Maslow's hierarchy of needs, and determinism. Multiple methods of research are used in this article, including surveys, data analysis and reports. Cyberpsychology is demonstrated in this article by the process of victimization such as being hooked on by fake links drawing on one's psychological needs. "Click this link to instantly gain 500 followers!" Draws from a psychological need for belonging. In Maslow's hierarchy of needs, two parts of the pyramid can increase someone's SNS usage, in turn increasing their risk for victimization. They are esteem needs, belonging and love needs.

One person may need to feel more accomplished in their life, this need can tempt one to engage in risky internet behaviors. For example, when they receive an email stating they won a $500 dollar gift card, they may not think twice, as having more money will boost their self-esteem. Belongingness and love can cause one to use social media more, as they grow their list of Facebook friends and continuously engage with others. Social media responds heavily to a human's need for belonging and engagement. Finally, determinism describes how human behavior is caused by preceding events. Prior victimization causing an increased fear of recurring victimization is a primary example of this.

Marginalized Group

A marginalized group that can be affected by this increased sense of fear would be the elderly. Unfortunately, phone fraud is quite common as the elderly often fall victim to scammer's social engineering tactics. Examples of common tactics used in these frauds include guilt tripping, fear, impersonation, and much more that scammers use to steal thousands of dollars from their victims. Elderly people are also more likely to fall for several types of social media frauds, including fake advertisements, fake products, fake videos, malicious links, and more. According to the findings of this study, "prior victimization is found to increase fear of recurring victimization." *(Park, Y., & Vieraitis, L. M. (2021)* Since the elderly are prime targets of successful cyber-attacks, they are more than likely to have a sense of fear of re-victimization.

Another group of individuals would be those with mental disabilities and learning difficulties. It may be difficult for this group of people to maintain proper security awareness or learn effective cyber strategies due to their disabilities. An attacker could easily take advantage of this by manipulating them via email, phone, or through social media. These individuals could also fall victim to a different type of attack, cyberbullying. This can have a detrimental effect on one's mental health and self-esteem. These individuals' low resilience to cybercrime could make them a bigger target for these types of attacks.

This study contributes confirmation of one of its hypotheses that "greater SNS usage increases the risk of online victimization, leading to a greater fear of victimization on SNS." *(Park, Y., & Vieraitis, L. M. (2021)* This hypothesis is supported by the data gathered, and shows that the more one uses SNS, the more susceptible one is. I believe this could be due to the increased exposure to cyber risks when someone uses social media more frequently. Another contribution of this study is the finding that prior experiences of victimization on SNS significantly contribute to the fear of re-victimization. For example, if one person falls victim to a fake advertisement and loses one hundred dollars, they will be more fearful of any advertisement they come across on social media.

Conclusion

In conclusion, this study supports the idea that higher SNS usage contributes to a higher risk of cyber victimization. It also supports the idea that previous experience with cyber victimization causes an increased fear of re-victimization. This article utilized findings from "*Routine Activities Theory,"* which describes a theory of how crime occurs. It also used data from the "Korean Institute of Criminology," which administered surveys to 1,000 adolescents and adults who use SNS sites. This data combined helped to contribute to the confirmation of hypotheses created by this article. Diverse types of factors were also discussed outside of these studies, such as how one is many life factors can contribute to the overall usage of SNS and the subsequent risk of cyber victimization. This article also utilized three different scientific principles of sociology including determinism, skepticism, and relativism. It also uses concepts addressed in class such as multi-method research, cyberpsychology, Maslow's hierarchy of needs, and determinism. Data analysis, surveys, and utilization of different studies are some of the methods of research used in this article. If someone is a frequent user of social media or SNS, they should look at their current security posture, as the findings of this article support that they

are more likely to be victims. It is important to remain educated and alert to cybercrime, this study would not exist if there were not such a threat.

References

Park, Y., & Vieraitis, L. M. (2021). Level of engagement with social networking services and fear of online victimization: The role of online victimization experiences. International Journal of Cybersecurity Intelligence and Cybercrime, 4(2), 38-52. https://www.doi.org/10.52306/04020421TERZ5728)