International Journal of Cybersecurity Intelligence & Cybercrime

Volume 4 | Issue 2 Article 4

8-2021

Level of Engagement with Social Networking Services and Fear of Online Victimization: The Role of Online Victimization Experiences

ybercrime, fear of crime, online victimization, social networking services (SNS)

Recommended Citation

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

Park & Vieraitis (2021). *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(2), 38-52.

Level of Engagement with Social Networking Services and Fear of Online Victimization: The Role of Online Victimization Experiences

Yeonjae Park*, University of Texas at Dallas, U.S.A.
Lynne M. Vieraitis, University of Texas at Dallas, U.S.A.

Keywords: cybercrime, fear of crime, online victimization, social networking services (SNS)

Abstract:
Prior research indicates that fear of crime may lessen a person's quality of life by leading them to avoid participating in social activities. The current study explores the relationship between fear of online victimization and participants' levels of engagement with social networking services (SNS). Using data from a survey of 1,000 adolescents and adults aged 14 to 59 years, the direct relationship between the level of engagement on SNS and fear of online victimization and the indirect relationship through prior victimization were assessed. Findings show that the direct effect of the level of engagement on SNS on victimization experience was significant. In addition, the relationship between the level of engagement and the fear of victimization on SNS was significantly mediated through prior victimization experiences on SNS. These findings support the hypothesis that greater exposure on SNS increases online victimization, leading to a greater fear of victimization on SNS. Considering the large role SNS play in social activities and relationships, the findings are important for understanding how victimization impacts fear and may help inform policymakers how to help people stay engaged freely in socializing in a safer online environment.

Introduction

For the last two decades, social media sites have changed the way people build social networks and relationships with others, no longer limiting them to meeting people in person. This phenomenon marks a significant change in people's routine activities. Communicating through accounts on social networking sites (SNS) is a new type of social activity that allows people to connect with users who share similar personal or career interests, social activities, and backgrounds (Gao et al., 2010). A recent report revealed that more than half, 54 percent, of the world's population is active on SNS—a number that grew by 13.2 percent (or 490 million) between January 2020 and January 2021 (Kemp, 2021). In particular, 72.3 percent of the U.S. population was active on SNS, while 89.3 percent of the population in South Korea, from which data for the current study were gathered, was active on SNS in January 2021 (Kemp, 2021). SNS became popular in 1999 among South Koreans with the introduction of Cyworld, an SNS platform in South Korea, which more than half or 26 million of South Korea's population used (Hwang, 2011). Since 2019, Facebook has accounted for 29.1 percent of South Korea's market share, followed by Instagram (27.9 percent), YouTube (18.8 percent), and Twitter (3.8 percent) (Kwon, 2019).

*Corresponding author
Yeonjae Park, Program in Criminology and Criminal Justice, University of Texas at Dallas, 800 W. Campbell Road, GR 31, Richardson, TX 75080. U.S.A.
Email: yeonjae.park@utdallas.edu

As the popularity of SNS increases, various concerns regarding their use have emerged. One of the most significant issues is the indiscriminate exposure to crime and victimization. Cybercrimes include traditional crimes such as bullying, stalking, economic fraud, and identity theft committed in the virtual environment, as well as new types of crimes such as malware attacks, hacking, and fishing. Several studies have examined various forms of cybercrimes involving SNS, including cyberbullying (Brochado et al., 2017; Ryu, 2020), cyber-sexual harassment, cyber defamation (Marwick & Miller, 2014), and cyber-impersonation (Choi & Lee, 2017; Mann, 2009). Although estimates vary on the extent of victimization, research suggests that it is widespread. In their review of 159 studies on the prevalence of cyberbullying, Brochado et al. (2017) found that overall victimization prevalence varied from one percent to 61.1 percent. More specifically, among South Korean users, 52.4 percent of males and 44.3 percent of females reported that they were victims of cyberbullying in 2019 (Ryu, 2020). Interpersonal violence offenses, such as cyber-sexual harassment and cyber-impersonation, have also become increasingly problematic, especially among college students (Choi & Lee, 2017).

While victimization in cyberspace is a relatively new area of criminological research, the fear of crime has long been the subject of research on crime (Choi et al., 2021). Researchers have identified several risk factors associated with the fear of crime, including neighborhood characteristics (Brunton-Smith & Sturgis, 2011; Gainey et al., 2011), economic inequality and lack of investment in education and social protection (Vieno et al., 2013), and more recently, the consumption of social media (Intravia et al., 2017). In addition to ecological risk factors, studies have also considered exposure to victimization risk as a predictor of fear of crime. Findings suggest that exposure to risk as measured by victimization rates (Stafford & Galle, 1984) or experiencing victimization (Gainey et al., 2011) is associated with greater levels of fear of crime. Similarly, research on adolescents and bullying concluded that a bullying experience increased the odds of fear of being bullied at school and the magnitude of fear was greater than for individuals who had not been victimized (Bachman et al., 2011). Sironi & Bonazzi (2016) also found significant effects of being a victim of a burglary or assault within the last five years on lowering the level of perceived safety. A recent study comparing U.S. and Canadian college students' fear of crime, stalking, and sexual victimization significantly increased the odds of feeling unsafe on campus and in the community (Daigle et al., 2021).

While previous studies seem to support the impact of victimization experience on the fear of crime, some studies suggest the relationship may be more complicated. For example, Rengifo and Bolton (2012) found that greater exposure to public settings, which is a product of individuals' calculations of avoiding risky areas, lowered their fear of crime. Grubb and Bouffard's (2015) study of sexual victimization found that victimization as an adolescent did not impact the fear of crime as an adult. Research on fear of cybercrime, albeit limited, is also mixed. Some studies find support for the link between perceived risk of victimization and fear of online interpersonal victimization (Henson et al., 2013), online scams (Yu, 2014), and victimization on SNS (i.e., Facebook) (Higgins et al., 2008). Henson and colleagues (2013) focused on sexual solicitations, stalking, intimidation, and other forms of interpersonal violence from intimate partners, friends/acquaintances, and strangers. Perceived risk of victimization positively affected the fear of online victimization in all types of victim-offender relationships. Higgins et al. (2008) found that perceived risk predicts fear of online victimization through Facebook. Previous victimization experience has also been shown to increase fear of online victimization (Randa, 2013; Virtanen, 2017) and lead to avoidance behavior and feelings of reduced freedom in cyberspace (Brand & Wilsem, 2021). Randa (2013) investigated how prior cyberbullying experience affects fear of victimization on SNS, online gaming sites, and online communities among youths ages 12-18. The results demonstrated a significant association between the victimization experience and greater fear of online victimization.

Other studies suggest that fear of crime depends on the type of crime or perhaps the age of study participants. Yu (2014) found that perceived risk was a significant predictor of fear of online scams and cyberbullying but not computer viruses and digital piracy. Pereira et al. (2016) reported that only 8.7 percent of their sample of adolescents from Portugal who were harassed online repeatedly reported a greater fear than before the victimization.

Considering the widespread use of SNS, associated changes in routine activities, and the increasing risk of online victimization, more research is needed to understand the fear of cybercrime victimization. Understanding the relationship between SNS and fear of crime is important as the results may provide directions for interventions that improve the safety of cyberspace for citizens. The current study seeks to fill the gap in research by measuring fear of cybercrime victimization among SNS users with a nationally representative sample of South Korean residents. We focus on the exposure of risk and prior victimization as factors that lead to the fear of online victimization. The following section provides a discussion of routine activities theory, which provides the theoretical framework for our study of fear of online victimization. Next, we present our data and methodology. We conclude the paper with a discussion of our results and suggestions for future research.

Theoretical Framework

Routine Activities Theory

Developed by Cohen and Felson (1979), routine activities theory postulated that crime could only occur when three elements converge in time and space— motivated offenders, suitable targets, and the absence of capable guardians. Unlike many criminological theories that focus on the number of motivated offenders or changes in the strength of their motivations, routine activities theory postulated that the criminal inclinations of individuals are a given and that such inclinations do not directly lead to law-breaking activities (p. 589). Individuals make decisions about whether to perform illegal behaviors based on social situations or the circumstances created by the routine activities of people in everyday life. According to Cohen and Felson (1979), changes in crime rates may be explained in terms of the availability of targets and the absence of capable guardians.

Tests of routine activities theory have been applied to a wide range of crimes, including burglary, sexual assault, larceny, drug dealing, and economic crimes, and has generally received strong empirical support (Felson & Eckert, 2019). Recent research has expanded the application of routine activities theory to other emerging forms of crime, including cybercrime, that are related to changes in the way we work, socialize with others, and spend leisure time. As previously discussed, the proliferation of SNS has had a profound impact on our routine activities, especially as they relate to socializing with others. Moreover, online platforms have emerged as a new "space" in which motivated offenders, suitable targets, and guardians converge, making routine activities theory a suitable framework from which to study cybercrime.

Routine Activities Theory and Cybercrime

The fact that routine activities theory considered space, regardless of whether it meant terrestrial or virtual (Grabosky, 2001), has made it one of the most popular theories for explaining cybercrime. Although the "convergence of space and time," is relatively disorganized in cyberspace, constructs of the elements of the routine activities theory have been acknowledged as continuous when adapted to cybercrime (Yar, 2005).

Accordingly, researchers have tested this approach to explain cybercrime and victimization in the virtual world since the late 2000s. Studies that focus mainly on the role of guardians in online victimization vary in their measures of guardianship; thus, it is difficult to compare findings across studies. However, the inconsistency in the effects of guardianship may also imply that the concept of guardianship from routine activities theory may need to be modified when applied to online victimization. For example, Choi (2008) applied routine activities theory to examine the online behaviors of college students and the actions they took to protect against online victimization. The study found that individuals who used a technically capable guardian as measured by antivirus software, antispyware software, or firewall software had a lower likelihood of computer virus victimization. In contrast, those who were involved in risky behavior (e.g., downloading content, using unidentified websites) on the internet significantly increased their likelihood of virus victimization.

Other research has integrated online routine activities, such as online shopping, chatting, and banking, and measured guardianship as participants' computer skills and antivirus software programs (Bossler & Holt, 2009). Bossler and Holt (2009) examined the association between the amount of time respondents spent engaged in routine activities online, the presence of guardianship (e.g., antivirus, spybot, ad-aware software, and one's computer skills), and data loss from malware infections. The results showed that neither online routine activities nor protective measures were related to malware victimization and only partial support for applying routine activities theory to cyber victimization. Similarly, in a study of adolescent online victimization, Marcum et al. (2010) found no significant protective effects of capable guardianship on victimization when the guardianship was measured as persons in the room while using a computer and monitoring software activated by parents.

In addition to studies that emphasize the role that absence of guardians may play in online victimization, other studies have focused on the routine activities that increase exposure to risk (Hindelang et al., 1978). Although researchers employ different measures of exposure to risk depending on the type of victimization under study, in general, findings suggest that increased exposure online is associated with higher levels of victimization. Using data from a telephone survey conducted in 2004, Pratt et al. (2010) found that the number of hours respondents spent online and making purchases online significantly increased the likelihood of becoming a victim of internet fraud. Hutchings and Hayes (2009) also reported results that support the routine activity perspective in their study of phishing crimes. They found that individuals with high levels of computer/internet experience or internet banking experience had a greater chance of online victimization.

A study by Marcum et al. (2010) operationalized the exposure to motivated offenders by constructing measures of *general internet use*—hours and days spent online (p. 387) and *types of activities*—using email, instant messaging, online chat rooms, and social networking websites (p. 388). The findings demonstrated that increased exposure to motivated offenders increased the likelihood of victimization (i.e., receipt of sexually explicit material, receipt of non-sexual harassment, receipt of sexual solicitation). Similarly, a study using longitudinal data found that online shopping, participation in forums, and using SNS increased the risk of online threats (van Wilsem, 2011), while online shopping and visiting forums increased the risk of consumer fraud (van Wilsem, 2013). Another study examining cyberbullying among adolescents found that exposure to the crime was maximized when suitable targets used the internet frequently because they had more opportunities to provide their private information, such as photos or addresses (Mesch, 2009).

A study from Switzerland hypothesized that the frequency of activities performed online would represent the level of exposure to crime (Milani et al., 2020). The results demonstrated that regardless of crime type, people who regularly use the internet or SNS have a greater likelihood of victimization (Milani et al., 2020).

Lastly, another study defined the exposure to motivated offenders by measuring how often participants used dangerous sites, such as the dark web or online gambling sites, and how often they shared content and uploaded personal photos online (Mikkola et al., 2020). The researchers included all three elements from routine activities theory in their analysis and found frequent social media use was the only element significantly associated with online victimization in all four targeted countries (i.e., United States, Finland, Spain, South Korea). In contrast, sharing or uploading on SNS was not significantly correlated with victimization except in Spain. The consistency in results of previous studies suggests that exposure to risk during routine activities may be a significant predictive factor in explaining online victimization.

In sum, a number of studies have explored the relationship between the elements of routine activities theory and various forms of cybercrime. Although the theory has been popular among researchers studying online victimization, the results are somewhat mixed regarding the role of guardians and exposure to risk. In addition, there are some limitations to these studies that we seek to address. First, much of the research uses samples of college students and adolescents. Although internet use, particularly engagement with SNS, may be more prevalent among these age groups, internet use has become widespread across the population (Pew Researcher Center, 2021). Second, most studies, with some exceptions, use samples from the U.S. population. As previously noted, half of the world's population is active on SNS, and the rate of use among South Korean residents exceeds that of U.S. residents. Lastly, cybercrime researchers have not paid significant attention to the role that fear of victimization may play among SNS users. We seek to fill these gaps by examining the relationship between fear of online victimization and participants' levels of engagement with social networking services with data from a survey of 1,000 South Korean residents ages 14 to 59. The direct relationship between the level of engagement on SNS and fear of online victimization and the indirect relationship through prior victimization were assessed.

Hypotheses and Focus of the Current Study

In addition to the aforementioned limitations, there has been no detailed investigation on the interrelation between exposure to risk, personal victimization, and the fear of crime from the perspective of cybercrime. The current study aimed to explore whether there is a relationship between exposure to risk and the fear of cybercrime mediated by the victimization experience (see Figure 1). To address this research question, three hypotheses were proposed: 1) greater exposure to risk in SNSs increases the fear of cybercrime; 2) personal victimization experiences increase the fear of cybercrime; and 3) personal victimization experiences mediate the relationship between the level of exposure to risk and the fear of cybercrime.

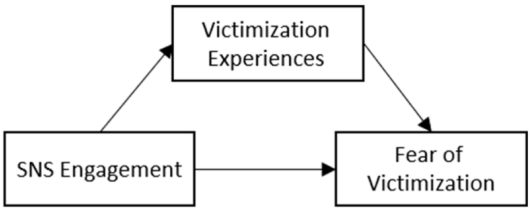

Figure 1. Structural Model

Methods

Data

Data for this study were collected by the Korean Institute of Criminology from July 2013 to August 2013 (Yoon & Park, 2014). Surveys were administered to 1,000 adolescents and adults who use at least one of four SNS sites (i.e., Facebook, Twitter, Kakao Story, Cyworld). The sites shared more than 90 percent of the SNS market in South Korea. Two-stage proportionate quota sampling, weighted by district, gender, and age population, was used to create a more representative sample. The gender ratio in the sample was relatively balanced (males: n = 510, 51.0%). The age range was 14 to 59 years, and the average age was 32.75 years (SD = 11.47). The highest percentage of the sample reported a high school diploma as their highest level of education (n = 441, 44.1%), and the most frequently reported average monthly income was ₩3,000,000 to ₩4,000,000, which corresponds to approximately 2,720 to 3,620 U.S. dollars (n = 331, 33.1%).

Independent Variables

Level of SNS Engagement was calculated as the number of open accounts respondents had with each SNS. Opening an account requires the user to provide personally identifying information to specific sites, thereby potentially exposing their information to others. When an individual opens multiple accounts, the information appears in various virtual spaces, leading to greater odds of being the target of criminal activity. As a result, the total number of SNS accounts indicates the individual's level of exposure to risk of online victimization. This is consistent with routine activities theory which suggests that proximity to motivated offenders, in this case, "virtual" proximity, increases an individual's exposure to risk as well as fear of victimization. Respondents had an average of 1.57 SNS accounts.

Victimization Experiences on SNS. The survey asked respondents to indicate whether they had experienced victimization on any of the four SNS sites within the past year. This measure consisted of 12 items:

> In the past year, someone using SNS has...
> 1) Repeatedly rejected me from friend requesting or joining groups.
> 2) Deceived me using fake advertisements that promise free giveaways or free coupons.
> 3) Deceived me using fake sites or links, causing me to suffer from personal information leaks.
> 4) Impersonated.
> 5) Used my personal information or photos.
> 6) Spread rumors or lies about me.
> 7) Defamed (without insults) and/or slandered me.
> 8) Insulted and/or threatened me.
> 9) Continuously sent me unwanted messages.
> 10) Continuously sent me messages, photos, and/or videos that made me scared or worried.
> 11) Continuously sent me obscene messages, photos, and/or videos.
> 12) Asked for sex in return for money or compensation.

The responses were rated with 1 (*Yes*) or 0 (*No*). The summed scores were used in the analysis, with higher scores indicating more frequent victimization in a given period. This measure demonstrated good internal consistency (α = .74).

Dependent Variable

Fear of Victimization on SNS. Respondents were asked to rate, using a 4-point Likert scale, how much they worry about victimization on the SNS sites. This measure included 12 items:

I worry that...
1) My privacy may be compromised when using SNS.
2) I may be deceived by someone and lose money or things when using SNS.
3) Someone may sexually harass me when using SNS.
4) Someone I know on SNS may sexually harass me in real life.
5) Someone I know on SNS may defame me and/or insult me.
6) Someone may spread rumors and/or lies about me on SNS.
7) My personal information may be compromised when using SNS.
8) Someone may impersonate me on SNS.
9) Someone may deceive me and/or attack my phones and/or computers.
10) Someone I know on SNS may continuously send unwanted messages.
11) Someone may steal my money and/or things using my information exposed when using SNS.
12) Someone may break into my house using my information exposed when using SNS.

The scale ranged from 0 (*Not afraid at all*) to 3 (*Afraid a lot*). The average score was used, with higher scores reflecting a greater fear of experiencing victimization on SNS sites. The items showed good internal consistency (α = .91).

Control Variables

The study included gender, age, highest level of education, and monthly average income as control variables. Gender was categorized as 0 (*Female*) or 1 (*Male*). The ages of the respondents were added as a continuous variable (ages 14 through 59). The highest level of education was coded from 1 (*Elementary school*) to 5 (*Beyond graduate*) and 6 (*Ineducation*). The monthly average income was included as a categorical variable, ranging from 1 (*Less than ₩1,000,000*) to 8 (*More than ₩7,000,000*). Descriptive statistics for the variables included in the multivariate analysis are shown in Table 1.

Table 1. Descriptive Statistics (N=1,000)

Variables	Mean	Std. Dev.	Min	Max
Gender (Male = 1)	0.51	0.50	0	1
Age	32.75	11.47	14	59
Highest Level of Education	3.57	1.05	1	6
Monthly Average Income	4.56	1.26	1	9
SNS Engagement	1.57	0.82	1	6
Victimization Experience	0.37	1.10	0	34
Fear of Victimization	1.09	0.50	0	2.83

Analytical Strategy

This study employed an ordinary least squares (OLS) regression analysis based on the path analysis to examine the mediation model. OLS regression is appropriate because it conducts the mediation analysis simultaneously (Fairchild & MacKinnon, 2009). The independent variable, SNS engagement, and the mediating variable, SNS victimization experience, are included in one model to examine mediating effects on the outcome variable. The mediation can be identified after confirming the direct association between the variables. We assessed the direct effects between 1) the level of engagement on SNS and victimization experiences and 2) victimization experiences on SNS and fear of victimization on SNS. Next, we examined the indirect effects of the hypothesized model (Figure 1). The control variables were included in all of the analyses. We used STATA to conduct the analyses.

Results

The bivariate correlations between all the variables are presented in Table 2. The dependent variable, which was the fear of victimization on SNS, was positively correlated with the level of engagement on SNS (r = .094, p < .01) and victimization on SNS (r = .080, p < .05). However, it was negatively correlated with gender (r = -.137, p < .01) and income (r = -.083, p < .01). The independent variable—the level of engagement on SNS—was positively correlated with victimization experiences (r = .170, p < .01). In contrast, age (r = -.239, p < .01) and education (r = -.080, p < .05) were negatively correlated with SNS engagement levels.

Table 2. Bivariate Correlations Matrix Among Variables (N=1,000)

	1	**2**	**3**	**4**	**5**	**6**	**7**
(1) Fear of Victimization	1						
(2) SNS Engagement	.094**	1					
(3) Gender	-.137**	.003	1				
(4) Age	-.002	-.239**	-.016	1			
(5) Education	.036	-.080*	.084**	.399**	1		
(6) Income	-.083**	.046	.001	.026	.179**	1	
(7) Victimization Experience	-.080*	.170**	.077*	-.103**	-.012	-.012	1

Note: p< .05, p< .01***

Victimization experiences on SNSs and the fear of victimization on SNSs are known to be highly related. To test for collinearity, we examined the variance inflation factor score; it did not exceed 1.00 (VIF=1.00). Thus, collinearity between these two variables was very low (Hair et al., 1995).

Mediating Effects of Victimization Experience on SNS

Table 3 demonstrates the direct effect of the level of SNS engagement on victimization. The level of SNS engagement had a significant effect on victimization on SNS (β = .20, p < .001). The right column in Table 3 further shows the direct effects of SNS engagement and victimization experiences on SNS on the fear of

victimization on SNS. All three variables were examined in one model, and the level of engagement on SNS was positively associated with the fear of victimization on SNS (β = .68, p < .01). The direct effect of the level of SNS engagement on the fear of victimization, which was one of the key estimates calculating indirect effects, was also significant (β = .43, p < .05). The results of control variables regressed on fear of victimization on SNS were as follows: gender (β = -1.82, p < .001), age (β = -.00, p > .05), education level (β = .42, p < .05), and income (β = -.48, p < .01).

Table 3. Direct Effects Model

Direct Effects										
	Victimization Experience					Fear of Victimization				
	β	S.E.	p	[95% C.I.]		β	S.E.	p	[95% C.I.]	
Victimization Experience						.43	.18	.019	.07	.79
SNS Engagement	.20	.04	.000	.12	.28	.68	.24	.004	.21	1.15
Gender	.15	.07	.024	.02	.28	-1.82	.38	.000	-2.56	-1.07
Age	-.01	.00	.013	-.01	.12	-.00	.02	.980	-.04	.04
Education	.05	.03	.116	-.01	.12	.42	.20	.034	.03	.82
Income	-.02	.03	.407	-.07	.03	-.48	.15	.002	-.78	-.18

Finally, Table 4 shows the indirect effects of the hypothesized model. Victimization experiences on SNS were identified as a significant mediator between the level of engagement and the fear of victimization on SNS (ß = .09, p < .05). The result equates to the product of the path coefficients between the independent variable and the mediator, and the second path coefficient between the dependent variable and the mediator.

Table 4. Indirect Effects Model

Indirect Effects					
	Fear of Victimization				
	β	S.E.	p	[95% C.I.]	
Victimization Experience					
SNS Engagement	.09	.04	.035	.01	.16
Gender	.06	.04	.104	-.01	.14
Age	-.00	.00	.089	-.01	.00
Education	.02	.02	.192	-.01	.06
Income	-.01	.01	.434	-.03	.01

Discussion

Considering the widespread use of SNS in our routine activities of work, family, and leisure time, understanding the factors associated with fear of victimization is an important topic of research. This study examines the association between the level of engagement in SNS and fear of victimization using a routine activities theoretical framework. According to routine activities theory, crime occurs when motivated offenders and suitable targets converge in the absence of capable guardians. As our day-to-day activities change in response to advances in technology, our exposure to the risk of criminal victimization has shifted to include the virtual world. Thus, fear of crime is no longer restricted to physical space but has expanded to include virtual spaces.

We hypothesized that higher levels of engagement on SNS, which indicates greater exposure to risk, would increase fear of crime on SNS. In addition, we included victimization experiences as a mediator between exposure to crime and fear of crime on SNS, hypothesizing that prior victimization increases levels of fear more than engagement alone. We controlled the effects of social and demographic characteristics, such as age and gender, to examine the vulnerability and victimization model's general mechanism. Prior research has not devoted significant attention to the fear of cybercrime victimization. The current study contributes to the study of cybercrime by examining fear of victimization on SNS using a nationally representative sample of South Korean residents. Several important findings are discussed.

First, our analyses indicated that the level of engagement on SNS had a positive effect on victimization and the fear of victimization on SNS. Thus, respondents with a greater number of SNS accounts reported higher levels of victimization and higher levels of fear of crime on SNS. Although these findings were consistent with our hypotheses, few studies have found empirical evidence to support this association. For instance, a study on the relationship between SNS usage time and the fear of crime on SNS showed that usage time had no significant effect on the fear of victimization or victimization experiences (Lee et al., 2019). However, Lee and colleagues' measure of exposure to risk on SNS, time spent on SNS or duration of exposure, differed from our measure, i.e., the number of accounts or extent of exposure, suggesting that different forms of risk exposure can influence the fear of crime. The inconsistency in findings may be attributable to the differences in measures—the extent of SNS usage (i.e., using various accounts and SNS sites) versus the duration (i.e., spending more time on SNS). More detailed research is needed to investigate the extent of SNS usage. For example, future studies can examine the number of accounts on one SNS site or count the number of sites a respondent uses.

Second, experiences of victimization on SNS significantly affected the fear of victimization. This relationship between victimization experiences and the fear of crime was in line with many previous studies. However, less is known regarding cybercrime specifically. Though this study discovered that such a relationship could be extended to crime on SNS, there is still a need to specify the type of cybercrime on SNS sites. Similar to other offline crimes, cybercrime on SNS can have various components. For instance, cyberbullying on SNS sites involves an interpersonal component, while hacking or identity theft does not require interpersonal contact (Virtanen, 2017). Since different crime components have different impacts on the fear of crime (Skogan & Maxfield, 1981), the effect sizes in this association can differ based on the types or components of crime the respondents experienced.

Finally, victimization experiences mediated the relationship between the level of SNS engagement and the fear of victimization on SNS. All three paths were significant and in the expected direction. We concluded that higher levels of engagement on SNS are associated with a greater number of victimization experiences, resulting in increased fear of crime on SNS. Effect sizes further demonstrated that the direct effects of the level of engagement on fear of victimization were greater than were prior victimization experiences. This result is interesting since one would expect prior victimization experiences to increase levels of fear more so than level of engagement on SNS. It is possible that the timing of the victimization experience might have impacted the effect size. Analyzing the data that specified conditions would help examine the mechanism beyond the present findings. It is also possible that individuals are more afraid of situations they are aware of, e.g., "I know that cyberbullying occurs on SNS," but have never experienced, e.g., "I have never been a victim of cyberbullying." For instance, Hirtenlehner (2008) suggested that the fear of crime projects general anxieties that are brought on from social changes. He explained that such feelings from the uncertainties are diffused to crime, which makes the fear of crime reflect a feeling of insecurity. Additionally, individuals who experienced victimization online may have reduced fear because they already dealt with it.

Policy Implications

The current study started with an idea that SNS users are not aware of how much information they are providing when they activate an account. Activating an account on SNS requires users to upload personally identifying information such as their date of birth, phone number, email address, relationship status, and other information such as political views. When this information is combined with the content that the user has read or liked online, the user's job or physical address, which he or she has never submitted to the site, can be determined. Creating multiple accounts across SNS, can increase exponentially the user's exposure to risk of victimization by motivated offenders who seek criminal opportunities online. However, many SNS users are unaware of how much information they actually provide when they activate an account (Acquisti et al., 2015; Obar & Oeldorf-Hirsch, 2020; Perrin, 2018; Smith, 2018).

The results of our study showed that high engagement in SNS sites by creating multiple accounts increased the fear of cybercrime via victimization experiences. Understanding fear of crime is important as research has demonstrated that the fear of crime can have harmful effects on people's physical and mental health (Pearson & Breetzke, 2014). According to Yoon and Park (2014), when people experience victimization on SNS, they often wonder "where, again, the personal information leak happened" (p. 173). These questions suggest that SNS users are vulnerable to cybercrime and that SNS providers provide insufficient protection.

Although users give permission to SNS providers to keep their data, users often do not know how these data are managed. Butler et al. (2011) pointed out that users are unaware of the changes in privacy policies and how they may affect their settings in SNSs. Policies that require stricter limits among SNS providers on collecting personal data and greater transparency in using personal data should be implemented to reduce users' risk of exposure on SNS. In particular, the policies should urge SNS providers to 1) give "exposure awareness" to the users and 2) allow users to easily make decisions regarding their personal information and the use of this information (Kapadia & Lee, 2016).

Policies that strengthen the security of personal information and the safety of users in online platforms should reduce various forms of cybercrime. In addition, these policies may also lessen the fear of victimization. Reducing fear of crime has led to changes in the routine activities of residents in some communities leading them to socialize and interact in public spaces (Lee et al., 2016; Kaplan & Chalfin, 2021). In theory, changes to online platforms should reduce the fear of online victimization and help foster the participation of people in online spaces.

Limitations and Future Research

We acknowledge several limitations in our study. First, although this study used a probability sampling method to acquire generalizability within South Korea, this sample does not reflect the populations of other countries. Second, temporal issues arise with the nature of cross-sectional data. While our hypotheses are theoretically grounded and empirically supported by the literature on cybercrime, we cannot determine the direction of causality between SNS engagement level, victimization experiences, and fear of cybercrime. Longitudinal investigations are needed to clarify such associations. Third, previous studies have demonstrated several ways to measure the exposure to risk (e.g., amount of time spent on SNSs); thus, we cannot be certain our measure is best. Future research should assess how measures of the concepts identified in routine activities theory are operationalized.

Conclusion

In this paper, we employed the routine activities theory to examine empirically how engagement with SNSs via the creation of multiple accounts is related to the fear of cybercrime and whether the relationship is mediated by victimization experiences on SNSs. The main findings indicated that the level of engagement in SNSs directly affected the victimization experience. In addition, the association between the level of engagement in SNSs and the fear of victimization on SNSs was significantly mediated via prior victimization experiences on SNSs. The results suggest that it is important not only to study the various types of crimes in cyberspace, but also to focus on the exposure to risk and the potential effects of victimization. Considering the significant role SNSs play in social activities and relationships, the findings are important for understanding how victimization impacts fear and may help to inform policymakers on how to help people stay engaged in a safer online environment.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Bachman, R., Randolph, A., & Brown, B. L. (2011). Predicting perceptions of fear at school and going to and from school for African American and White students: The effects of school security measures. *Youth & Society, 43*(2), 705-726.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Brands, J., & van Wilsem, J. (2021). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology, 18*(2), 213-234.

Brochado, S., Soares, S., & Fraga, S. (2017). A scoping review on studies of cyberbullying prevalence among adolescents. *Trauma, Violence, & Abuse, 18*(5), 523-531.

Brunton-Smith, I., & Sturgis, P. (2011). Do neighborhoods generate fear of crime? An empirical test using the British Crime Survey. *Criminology, 49*(2), 331-369.

Butler, E., McCann, E., & Thomas, J. (2011). Privacy setting awareness on Facebook and its effect on user-posted content. *Human Communication, 14*(1), 39-55.

Choi, J, Kruis, N.E., & Choo, K.S. (2021). Explaining fear of identity theft victimization using a routine activity approach. *Journal of Contemporary Criminal Justice, 37*, 406-426.

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and of fending using cyber-routine activities theory. *Computers in Human Behavior, 73*, 394-402.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review,* 588-608.

Daigle, L. E., Hancock, K., Chafin, T. C., & Azimi, A. (2021). US and Canadian College Students' Fear of Crime: A Comparative Investigation of Fear of Crime and Its Correlates. *Journal of Interpersonal Violence.* https://doi.org/10.1177/08862605211001477

Fairchild, A. J., & MacKinnon, D. P. (2009). A general model for testing mediation and moderation effects. *Prevention Science, 10*(2), 87-99.

Felson, M. & Eckert, M.A. (2019). *Crime and Everyday Life, 6th edition.* Thousand Oaks, CA: Sage.

Gainey, R., Alper, M., & Chappell, A. T. (2011). Fear of crime revisited: Examining the direct and indirect effects of disorder, risk perception, and social capital. *American Journal of Criminal Justice, 36*(2), 120-137.

Gao, Q., Rau, P. L. P., & Salvendy, G. (2010). Measuring perceived interactivity of mobile advertisements. *Behaviour & Information Technology, 29*(1), 35-44.

Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? Social & Legal Studies, 10, 243-249.

Grubb, J. A., & Bouffard, L. A. (2015). The influence of direct and indirect juvenile victimization experiences on adult victimization and fear of crime. *Journal of Interpersonal Violence, 30*(18), 3151-3173.

Hair, J. F., Jr., Anderson, R. E., Tatham, R. L. & Black, W. C. (1995) *Multivariate Data Analysis* (3rd ed.), NY: Macmillan.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice, 29*(4), 475-497.

Higgins, G. E., Ricketts, M. L., & Vegh, D. T. (2008). The role of self-control in college student's perceived risk and fear of online victimization. *American Journal of Criminal Justice, 33*(2), 223-233.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization.* Cambridge, MA: Ballinger.

Hirtenlehner, H. (2008). Disorder, social anxieties and fear of crime. Exploring the relationship between in civilities and fear of crime with a special focus on generalized insecurities. In H. Kury (Ed.), *Fear of crime – Punitivity. New developments in theory and research* (pp. 127–158). Bochum, Germany: Brock meyer.

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimisation: who gets caught in the 'net'?. *Current Issues in Criminal Justice, 20*(3), 433-452.

Hwang, J. (2011). Will the Cyworld make comeback?. *Maeil Business Newspaper*. Retrieved from https:// www.mk.co.kr/news/business/view/2011/09/598392/

Intravia, J., Wolff, K. T., Paez, R., & Gibbs, B. R. (2017). Investigating the relationship between social media consumption and fear of crime: A partial analysis of mostly young adults. *Computers in Human Behavior, 77*, 158-168.

Kapadia, A., & Lee, A. J. (2016). *Improving privacy through exposure awareness and reactive mechanisms.* CHI 2016 Workshop on Bridging the Gap between Privacy by Design and Privacy in Practice. ACM.

Kaplan, J., & Chalfin, A. (2021). Ambient lighting, use of outdoor spaces and perceptions of public safety: evidence from a survey experiment. *Security Journal*, 1-31. https://doi.org/10.1057/s41284-021-00296-0

Kemp, S. (2021). *DIGITAL 2021: GLOBAL OVERVIEW REPORT.* Singapore: DataReportal. Retrieved from https://datareportal.com/

Kwon, Y. (2019). 9-in-10 adults using SNS...Preferred SNS platform by age. *Digital Chosun*. Retrieved from http://digitalchosun.dizzo.com/site/data/html_dir/2019/03/18/2019031880179.html

Lee, J. S., Park, S., & Jung, S. (2016). Effect of crime prevention through environmental design (CPTED) measures on active living and fear of crime. *Sustainability, 8*(9), 872.

Lee, S. S., Choi, K. S., Choi, S., & Englander, E. (2019). A test of structural model for fear of crime in social networking sites. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(2), 5-22.

Mann, B. L. (2009). Social networking websites–a concatenation of impersonation, denigration, sexual aggressive solicitation, cyber-bullying or happy slapping videos. *International Journal of Law and Information Technology, 17*(3), 252-267.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior, 31*(5), 381-410.

Marwick, A., & Miller, R. (2014). *Online harassment, defamation, and hateful speech: A primer of the legal landscape* (Fordham Center on Law and Information Policy Report No. 2). Retrieved from http://ssrn.com/abstract=2447904.

Mesch, G. S. (2009). Parental mediation, online activities, and cyberbullying. *Cyber Psychology & Behavior, 12*(4), 387-393.

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., ... & Paek, H. J. (2020). Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context. *International Journal of Offender Therapy and Comparative Criminology*, 0306624X20981041.

Milani, R., Caneppele, S., & Burkhardt, C. (2020). Exposure to Cyber Victimization: Results from a Swiss Survey. *Deviant Behavior,* 1-13.

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128-147.

Pearson, A. L., Breetzke, G. D. (2014). The association between the fear of crime, and mental and physical wellbeing in New Zealand. *Social Indicators Research, 119*(1), 281–294.

Pereira, F., Spitzberg, B. H., & Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior, 62*, 136-146.

Perrin, A. (2018). *Americans are changing their relationship with Facebook.* Pew Research Center. https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Randa, R. (2013). The influence of the cyber-social environment on fear of victimization: Cyber bullying and school. *Security Journal, 26*, 331-348.

Rengifo, A. F., & Bolton, A. (2012). Routine activities and fear of crime: Specifying individual-level mechanisms. *European Journal of Criminology, 9*(2), 99-119.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169.

Ryu, E. (2020). Cyberbullying risks for 40s and 50s rise. *Itchosun*. Retrieved from http://it.chosun.com/site/data/html_dir/2020/10/13/2020101300491.html

Sironi, E., & Bonazzi, L. M. (2016). Direct victimization experiences and fear of crime: A gender perspective. *Peace Economics, Peace Science and Public Policy, 22*(2), 159-172.

Skogan, W. G., & Maxfield, M. G. (1981). *Coping with crime: Individual and neighborhood reactions* (Vol. 124). Beverly Hills, CA: Sage Publications.

Smith, A. (2018). *Many Facebook users don't understand how the site's news feed works*. Pew Research Center. https://www.pewresearch.org/fact-tank/2018/09/05/many-facebook-users-dont-understand-how-the-sites-news-feed-works/

Stafford, M. C., & Galle, O. R. (1984). Victimization rates, exposure to risk, and fear of crime. *Criminology, 22*(2), 173-185.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115-127.

Van Wilsem, J. (2013). 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168-178.

Vieno, A., Roccato, M., & Russo, S. (2013). Is fear of crime mainly social and economic insecurity in disguise? A multilevel multinational analysis. *Journal of Community & Applied Social Psychology, 23*(6), 519-535.

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law, 24*(3), 323-338.

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407-427.

Yoon, H., & Park, S. (2014). *Cybercrime in social networking services and criminal justice responses.* Korean Institute of Criminology.

Yu, S. (2014). Fear of cybercrime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology, 8*(1), 36-46.