경영학석사학위논문

A Lifestyle-Routine Activity Theory (LRAT) Approach to Cybercrime Victimization:

Empirical Assessment of SNS Lifestyle Exposure Activities

생활양식-일상활동이론(LRAT)으로 바라본 사이버범죄 피해:

SNS 생활양식 노출 활동에 대한 정량적 연구

2018 년 2 월

서울대학교 대학원

경영학과 경영정보시스템전공

최 지 선

Abstract

The Internet and its overwhelming possibilities and applications have changed individuals' lifestyles related to socializing, working, and spending leisure time. Social networking sites (SNSs) such as Facebook or Instagram are ideal settings for interacting with others, and unfortunately, are also ideal settings for motivated offenders to commit cybercrimes, thus making individuals more vulnerable. The purpose of this study is to investigate the occurrence of cybercrime victimization, specifically cyber-harassments, cyber-impersonation, and hacking. Self-report surveys collected from a sample of 100 respondents were examined using a logistic regression analysis to determine possible relationships between SNS lifestyle exposure activities and the cybercrime victimization. The results indicate moderate support for the application of lifestyle-routine activity theory (LRAT) to cybercrime victimization. Possible educational and managerial implications, as well as suggestions for future research, are discussed.

Keywords: lifestyle-routine activity theory (LRAT), lifestyle, cybercrime, cyber victimization, social networking sites (SNS), online user behavior

Student Number: 2016-20634

Table of Contents

1. Introduction

As the Internet population has grown to more than half of the world's population (Wearesocial, 2017) and technology has advanced, the way people communicate has also evolved. Recently, of all the online communication platforms, social networking sites (SNSs) have gained much popularity, especially among young adults as they provide cheaper and more interactive communication means (Kokkinos, 2017). Despite the beneficial outcomes they provide, various hazards have also been found to accompany this "wave of digital progressivism" (K. Choi, & Lee, J. R., 2017). SNS users release personal information and pictures online without realizing that their actions may lead to increased vulnerability to cyber-harassment and identity theft (Shin, 2010). This is the reason for more researchers to explore the cause or the consequences of SNS usage and cybercrime victimization.

Previous research on this subject shows the correlation between SNS users activities and their chances of being victimized online. An earlier study conducted by Spitzberg and Hoobler (2002) found that 31% of undergraduate student participants experienced some kind of personal online victimization (Spitzberg, 2002). In a similar study conducted by Henson et al. (2011), 42% of social network users reported experiencing some form of interpersonal victimization online (Henson, 2011). A more recent study performed by Kokkinos & Saripanidis (2017) focusing on Facebook user activities shows that "the victim's behavior may enhance the chances of getting victimized." Although the victim's behavior may be an important element to consider, there seems to be a widely-mistaken assumption that only risky online activities have the ability to propel one's status as a potential cyber-victim. The classification of risky online behaviors has become unclear due to the convergence of diverse types of activities available on SNS. For example, one cannot simply judge an individual's act of exposing daily activities or expressing feelings and opinions on SNS to be a risky behavior since it is the main feature provided by most of the SNS platforms.

Former studies that have assessed the influence of SNS activities on cybercrime victimization focused on different types of cybercrimes. The categorizations and definitions of cybercrimes vary depending on the researcher's focus. For example, some researchers like Yar (2005) made a distinction between 'computer-assisted crimes' and 'computer-focused crimes'. Computer-assisted crimes are characterized as crimes that have existed before the internet, but have taken on new life in cyberspace (e.g., theft, fraud), whereas, computer-focused crimes are crimes that have emerged with the creation of the Internet (e.g., hacking, website defacement). Other researchers such as Wall (2001) subdivided 'cybercrime' into four established legal categories: cyber-trespass, cyber-deceptions, and thefts, cyber-pornography, cyber-violence. This study focuses on two of Wall's categories, which are 'cyber-trespass' and 'cyber-violence'. Specific types of cybercrimes are violent and sexual cyber-harassment, which refers to 'cyber-violence', and cyber-impersonation and hacking, which refers to 'cyber-trespass'.

The current study, thus, explores SNS activities to find answers to two main research questions: *1. Are people who use SNS more often and share their daily activities through SNS more likely to be victimized by cybercrimes? 2. While using SNS, would stricter privacy settings reduce individuals being victimized by cybercrimes?* The theoretical approach mainly refers to the Lifestyle-Routine Activity Theory (LRAT), which is an integrated theory of Hindelang et. al's (1978) Lifestyle Exposure Theory and Cohen & Felson's (1979) Routine Activity Theory, found in most of the related literature. LRAT is a representative theory in this subject area stating that victimization is a result of individual routine activities and behaviors (lifestyle exposure activities), which increase exposure to motivated offenders and decrease exposure to capable guardianship (L. E. Cohen, Kluegel, J. R., & Land, K. C., 1981). The purpose of this study is to examine whether SNS lifestyle exposure activities increase the likelihood of cybercrime victimization. Data were collected through self-report surveys and analyzed with logistic regression due to the nature of dependent variables being binary (victimized or not victimized). Suggestions for future research have been made by elaborating on the results and several discussion points.

2. Theoretical Background and Hypotheses

Theoretical Framework

Previous studies that have mainly focused on identifying the factors which increase the risk of cybercrime victimization state that the victim's behavior may be as vital as the offenders' characteristics (Elias, 1986). A number of studies have applied the Victim Precipitation Model (VPM) as a framework in order to examine how a victim's behavior is associated with being victimized online (Cappadocia, 2013; Dredge, 2014; Hinduja, 2008; Peluchette, 2015; Staksrud, 2013; Walrave, 2011). According to this criminology framework, traditionally, there are certain spatial and temporal conditions in which initiate some type of action that results in their subsequent victimization (Miethe, 1994). Overall, these studies consistently indicate that there is a connection between the victim's behavior and the risk of being victimized online (Peluchette, 2015).

Several theories mainly focusing on the victims' characteristics and conditions have been introduced (L. E. Cohen, & Felson, M., 1979; L. E. Cohen, Kluegel, J. R., & Land, K. C., 1981; Hindelang, Gottfredson, & Garofalo, 1978) in order to explain the factors that precipitate victimization. Cohen et al.'s (1981) lifestyle and routine activity theory (LRAT), a widely used theoretical approach to study criminal victimization, is the integrated theory of Hindelang et al.'s (1978) lifestyle exposure theory and Cohen & Felson's (1979) routine activity theory. This integrated theory states that victimization is a result of individual routine activities and behaviors, which increase exposure to motivated offenders and decrease exposure to capable guardianship (L. E. Cohen, Kluegel, J. R., & Land, K. C., 1981). Before explaining LRAT, it is necessary to understand each theory, which became the foundations of LRAT, and how they are integrated into one.

Lifestyle Exposure Theory

Lifestyle exposure theory posits that an individual's routine behaviors and daily lifestyles, referring to routine activities, are what makes one a suitable target for criminal victimization (Hindelang et al., 1978). Hindelang et al. mainly argue that individuals who have different demographic and socioeconomic characteristics may have different role expectations and structural constraints that affect lifestyle choices available to them, such as where they live, with whom they associate, or how they are entertained, which in turn expose them to different risks of victimization (Hindelang et al., 1978). This can be interpreted such that some individual lifestyles put people in riskier situations than others which eventually create criminal opportunities facilitating criminal victimization (K. Choi, 2008).

Routine daily activities defined by Hindelang et al. (1978) include both vocational activities (work, school, keeping house, etc.) and leisure activities. Depending on the individual characteristics, their vocational and leisure activities vary on a large scale. According to Hindelang et al. (1978), people who spend more time in public places, especially during the night, and with non-family members are more likely to be victims of personal crimes. In addition, being in public places is directly related to the lifestyles of individuals (Yucedal, 2010).

Routine Activity Theory

Cohen and Felson's (1979) routine activity theory, an expansion of the lifestyle-exposure theory, explains how crime occurs with the convergence of three essential elements which are motivated offenders, a suitable target, and absence of capable guardianship. When one of these three elements is absent, crime does not occur (L. E. Cohen, & Felson, M., 1979; Messner, 1987; Miethe, 1994). However, according to the theory, when all three converge, crime occurs. This means that if a suitable target is exposed to a motivated offender in the absence of a capable guardian that could potentially prevent the offender from committing a crime, there is a high possibility of crime occurring (L. E. Cohen, & Felson, M., 1979).

In most of the social science research, the concept of a motivated offender is given, and therefore, is not included as a measured variable (Phillips, 2015). Previous studies more frequently examine variables that may affect an increase or decrease in suitable targets and capable guardians. According to Felson (1998), target suitability is likely to reflect four main criteria: the value of crime target, the inertia of crime target, the physical visibility of crime target, and the accessibility of crime target (VIVA).

Lifestyle and Routine Activity Theory

The two theories explained above, the lifestyle exposure theory (Hindelang et al., 1978) and the routine activity theory (L. E. Cohen, & Felson, M., 1979), are integrated as the lifestyle and routine activity theory (LRAT) (L. E. Cohen, Kluegel, J. R., & Land, K. C., 1981). According to Ngo & Paternoster (2011), they both "attempt to explain how routine activities of the victims are related to the risk of victimization and how criminal opportunities develop out of the routine activities of everyday life" (Kokkinos, 2017).

LRAT is based on the idea that individuals may encounter criminal events depending mainly on the kind of places (setting) in which an individual spends their free time, and what kind of activities they engage in during their free time (Svensson, 2010). The routine activity concept of a suitable target incorporates the lifestyle theory concepts of vocational and leisure activities. According to LRAT, an individual's lifestyle routine activities and behaviors are what defines him or her to be a suitable target (L. E. Cohen, Kluegel, J. R., & Land, K. C., 1981).

Cohen et al.'s theory (1981) includes the following major components: exposure to potential offenders, proximity to crime, guardianship, and target attractiveness. Originally, they are defined based on the relationships of each component with the physical/real world. First, the 'exposure to potential offenders' component refers to the physical visibility and accessibility of persons or objects to potential offenders at any given time or place. The second component 'proximity to crime' is defined as the physical distance between areas where potential targets of crime reside and areas where relatively large populations of potential offenders are found. The third component 'guardianship' is defined as the effectiveness of persons (e.g., housewives, neighbors, security guards) or objects (e.g., burglar alarms, locks, barred windows) in preventing violations from occurring, either by their presence alone or by some sort of direct or indirect action. The fourth component 'target attractiveness' is the material or symbolic desirability of persons or property targets to potential offenders, as well as the perceived inertia of a target against illegal treatment. Additionally, there are features of specific crimes that act to constrain strictly instrumental actions by potential offenders (L. E. Cohen, Kluegel, J. R., & Land, K. C., 1981).

The theoretical application of LRAT to cybercrime victimization, specifically on SNS platforms, will be discussed in the following section with the details of each component.

Theoretical Application to Cybercrime Victimization

Previous studies have used the routine activity theory or the integrated theory, LRAT, to explain the cybercrime victimization related to online activities (K. Choi, 2008; Ngo, 2011; Yar, 2005; Yucedal, 2010) and some have applied these assumptions in a number of empirical studies (Alshalan, 2006; K. Choi, 2008; Holt, 2009). These studies have set their research settings as the cyberspace as a whole. However, recent studies have incorporated the Social Networking Sites (SNSs) as a separate environment (Back, 2016; K. Choi, & Lee, J. R., 2017; Phillips, 2015) and some focused on the relationship between cybercrime victimization and specific SNS platforms such as Facebook (Dredge, 2014; Kokkinos, 2017; Peluchette, 2015). This study will mainly focus on the use of SNS, including Facebook but not limited to, and the users' SNS activities instead of investigating their online behaviors as a whole.

In order to explain the theoretical application of LRAT to cybercrime victimization, each of the major four components described in Cohen et al.'s (1981) study first needs to be dealt with independently. First, the current study assumes that proximity to crime is given, as with most of the previous studies (K. Choi, & Lee, J. R., 2017; Phillips, 2015), since the infinite and anonymous nature of the Internet is given. As the component 'exposure to potential offenders' is closely related to the proximity to crime, this is also assumed. Choi & Lee (2017) argue that "given the rise of digital technology, the physical convergence of potential offenders and victims in time and space are no longer quintessential elements to engender victimization (Eck, 2003; Holtfreter, 2008; Pratt, 2010)". Thus, this study mainly focuses on the other two components, which are 'target attractiveness' and 'capable guardianship'.

For 'target attractiveness', Cohen et al. (1981) state that individual routine daily behaviors and activities, in other words, lifestyle characteristics (including vocational and leisure activities), determine whether he or she is a suitable target or not. Former studies have introduced the risky online behavior as a concept of vocational and leisure activities. For example, Phillips (2015) conceptualized social networking itself as risky online behavior and Kokkinos & Saripanidis (2017) posited that a risky lifestyle on Facebook could include the time victims spend online, the number of Facebook friends, the Facebook content, etc. Choi & Lee (2017) assessed three variables – cyber risky SNS activities, cyber risky leisure activities, and cyber risky vocational activities – risky online behaviors. However, considering the particularity of SNS platforms, it is difficult to find a clear distinction between users' vocational, leisure, and risky activities within SNS. Therefore, this study does not distinguish the three but, instead, differentiates the types of routine activities using SNS. The different types of activities will be further explained in the hypothesis section.

For 'capable guardianship', former studies have mainly focused on physical or technological guardianship (virus and firewall software) in the case of cybercrime attacks such as malware or hacking (Yar, 2005; Yucedal, 2010). In the case of SNS guardianship, it is conceptualized as online privacy settings on personal networking sites (K. Choi, & Lee, J. R., 2017; Phillips, 2015). This study also considers SNS privacy settings as the capable guardianship on SNS.

Types of Cybercrime

Cybercrime can be defined as "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)"(Halder, 2011). According to Yar (2005), the term 'cybercrime' may refer to a range of illicit activities whose common distinction is the central role played by networks of information and communication technology (Phillips, 2015).

Yar (2005) further clarified classification between 'computer-assisted crimes' (those crimes that pre-date the Internet but take on a new life in cyberspace, e.g. fraud, theft, money laundering, sexual harassment, hate speech, pornography) and 'computer-focused crimes' (those crimes that have emerged in tandem with the establishment of the Internet and could not exist apart from it, e.g. hacking, viral attacks, website defacement) (Wall, 2001; Yar, 2005). The above definition may be socio-technically helpful, but it has a limited criminological utility. Wall's (2001) classification of cybercrime subdivided into four established legal categories (cyber-trespass, cyber-deceptions, and thefts, cyber-pornography, cyber-violence) seem to better describe cybercrime. This study will focus on 'cyber-trespass', which signifies crossing boundaries into other people's property and/or causing damage (e.g., hacking, defacement, viruses), and 'cyber-violence', which refers to doing psychological harm to, or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person (e.g., hate speech, stalking). Specific cybercrime variables and measures will be described in the methodology section.

Hypotheses

Based on the theoretical application to cybercrime, the following hypotheses are developed for this study:

H1: Individuals who expose their lifestyle via SNS activities are more likely to be victims of cybercrime.

- *H1a: Individuals who use SNS frequently are more likely to be victims of* *cybercrime.*

- *H1b: Individuals who share daily activities on SNS are more likely to be victims of cybercrime.*
- *H1c: Individuals who disclose preferences through SNS are more likely to be victims of cybercrime.*
- *H1d: Individuals who express their opinions or feelings are more likely to be victims of cybercrime.*

H2: Individuals who have stricter SNS privacy settings are less likely to be victims of cybercrime victimization.

Social networking sites create an environment for both positive and negative interaction with peers. While SNS, such as Facebook, have been found to enhance interpersonal relationships and build social capital, they have provided a place for cybercrime offending as well (Kowalski, 2014). As LRAT argues, the possibility of cybercrime offending is closely related to victims' behaviors on SNS. Peluchette et al. (2015) have found that "how individuals use social networking and the type of profile content they choose to post is likely to be influenced by the level of concern that they have for what others think of them but may also unknowingly be placing them at greater risk for cyberbullying" (Peluchette, 2015). Although their research focused on cyberbullying, there always is a possibility for other types of cybercrime.

Furthermore, studies have shown that self-disclosing through SNS could enhance the chances of victimization (Wilson, 2012) since those who disclose more personal information through SNS are more likely to become victims (Peluchette, 2015). Kokkinos & Saripanidis (2017) have defined ‘self-disclosure’ on SNS as the willingness to discuss personal information with other users on Facebook. Choi & Lee (2017) have included ‘expressing opinions and feelings through SNS’ as a measure of their ‘cyber risky SNS activities’ variable. As with the above research findings, this study assesses the influence of SNS use on cybercrime victimization (H1) via different types of SNS activities (H1a-H1d). H1c is added as SNS users also disclose their preferences by following or liking others’ contents/pages.

For H2, as Choi & Lee (2017) has stated, digital capable guardianship is conceptualized as online privacy settings on personal networking sites. Back’s (2016) study included security application on SNS as additional means of guardianship. However, this study only assesses the privacy settings on SNS as capable guardianship.

3. Research Design & Methodology

Research Model

Along with the hypotheses, Figure 2. depicts the research model in more detail with each hypothesis.

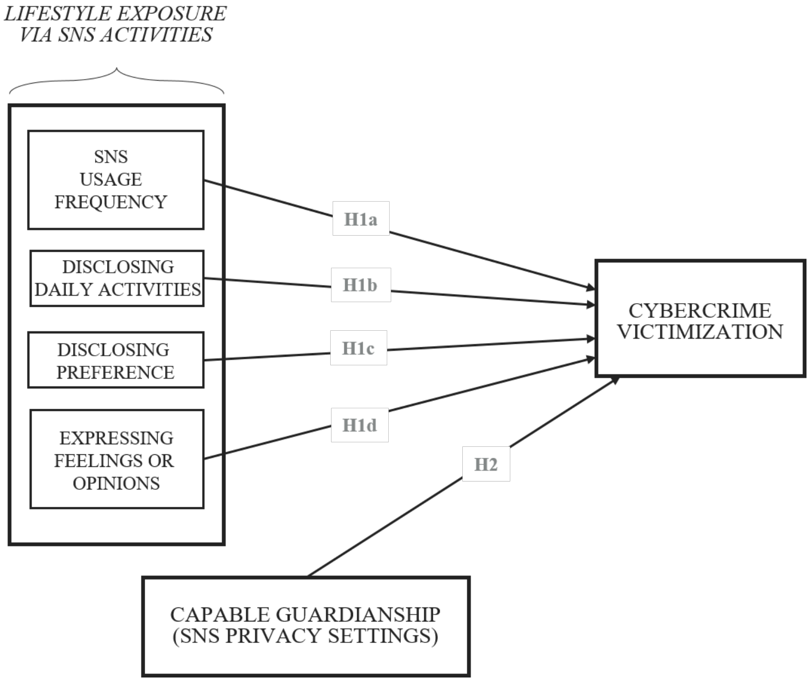

LIFESTYLE EXPOSURE VIA SNS ACTIVITIES
SNS USAGE FREQUENCY
DISCLOSING DAILY ACTIVITIES
DISCLOSING PREFERENCE
EXPRESSING FEELINGS OR OPINIONS
H1a
H1b
H1c
H1d
H2
CYBERCRIME VICTIMIZATION
CAPABLE GUARDIANSHIP (SNS PRIVACY SETTINGS)

Fig. 1 Research Model in Detail

Data and Sample

Data was collected from self-report surveys given to a random sample of respondents. Nonprobability sampling was done while age variance and occupation diversity were taken into consideration. 153 survey responses have been collected at first. Responses with error, such as missing or inconsistent responses, have been removed. Finally, a total of 100 respondents participated in the study, meaning a sample of 100 surveys were analyzed for this research project. Furthermore, the sample demographic characteristics are presented in Table 1. In the sections below, the detailed survey instruments regarding each variable are presented.

Demographic Characteristics	Categories	Study Sample (N=100)
Age	10 ~ 19 20 ~ 29 30 ~ 39 40 ~ 49 50 ~ 59 60 ~	1% (n=1) 55% (n=55) 27% (n=27) 0% (n=0) 12% (n=12) 5% (n=5)
Gender	Female Male	52% (n=52) 48% (n=48)
Occupation	Engineering / technician / IT-related Student Business management / finance Art / entertainment / sports Education / research / law / medical Other ___________	6% (n=6) 33% (n=33) 16% (n=16) 4% (n=4) 30% (n=30) 11% (n=11)

Table. 1 Demographic Characteristics of Sample

Independent Variables

There are five independent variables in total to be assessed regarding the relationships between SNS lifestyle exposure activities or capable guardianship and cybercrime victimization. Regarding the first measure of SNS usage frequency, six survey items were operationalized: (1) “SNS accounts subscribed in any SNS platform (Facebook/Instagram/KakaoStory/Naver Band/Twitter) (multiple responses available)”; (2) “most oftenly used SNS accounts on any SNS platform (Facebook/Instagram/KakaoStory/Naver Band/Twitter) (multiple responses available)”; (3) “use SNS at specific time or randomly”; (4) “how much time spent on SNS”; (5) “how many postings, including images and video clips, user uploads in a week”; (6) “how many comments user writes in a week.” The survey items chosen for this variable all pertain to how often one uses social networking. Respondents were asked to indicate their answer by selecting the box that best fit their feelings towards the given statements for (1) to (3). The responses for (1) and (2) were then separately counted by each individual. Responses for (3) were not used for the analysis. For statement (4), respondents were asked to state the minutes spent. For statements (5) and (6), respondents were required to write the numbers roughly. In order to integrate the responses as one variable measuring the SNS usage frequency (SNS_V1), all responses were summed up and then re-operationalized from scale 1 to 100. The scale represents a possible minimum score of 15 indicating a low level of SNS usage frequency, and a maximum score of 100 indicating a high level of SNS usage frequency. The mean score for SNS usage frequency variable was 40.27 with a standard deviation of 17.40.

The second measure of SNS lifestyle exposure activities consisted of two survey items that constituted daily activities through SNS: (1) “whether user shares daily activities through SNS”; (2) “what type of contents are mostly uploaded on user’s profile (multiple responses available)”. Respondents were asked to indicate their answer by answering ‘yes’ or ‘no’ to the given statement (1). For (2), the respondent could select several answers that match with their SNS contents. However, only the responses for (1) were analyzed for the variable measuring whether users disclose their daily activities through SNS or not (SNS_V2). The scale represents a possible minimum score of 0 indicating a low level of daily activities disclosure through SNS, and a maximum score of 1 indicating a high level of daily activities disclosure through SNS. The mean score for disclosing daily activities through SNS variable was 0.57 with a standard deviation of 0.50.

Regarding the third measure of SNS lifestyle exposure activities, two survey questions that constituted disclosing user preference through SNS activities were asked: (1) "Do you 'follow' the person/page that you are interested in?"; (2) "Do you 'like' the postings that you like or are interested in?" Respondents were asked to indicate their answer by answering 'yes' or 'no' to both given statements. In order to integrate the responses as one variable measuring whether the respondent discloses their preference via SNS activities (SNS_V3), all responses were summed up and then re-operationalized from scale 1 to 10. The scale represents a possible minimum score of 0 indicating a low level of preference disclosure through SNS, and a maximum score of 10 indicating a high level of preference disclosure through SNS. The mean score for preference disclosure through SNS variable was 7.65 with a standard deviation of 3.51.

The fourth measure of SNS lifestyle exposure activities consisted a survey item to create a variable that assesses whether the respondent expresses feelings/opinions through SNS (SNS_V4): "whether user expresses feelings/opinions through SNS". Respondents were asked to indicate their answer by answering 'yes' or 'no' to the given statement. The scale represents a possible minimum score of 0 indicating a low level of exposing feelings/opinions via SNS activities, and a maximum score of 1 indicating a high level of exposing feelings/opinions via SNS activities. The mean score for exposing feelings/opinions via SNS activities variable was 0.53 with a standard deviation of 0.50.

Regarding the fifth measure of SNS privacy settings, which measures the capable guardianship on SNS, a survey item was operationalized: "To what extent do you set your privacy settings?". Respondents were asked to indicate their answer by selecting the box that best fit their feelings towards the given statements ranging from "strongly disagree" to "strongly agree." The scale was 1 to 5 and the responses were analyzed as one variable constituting SNS privacy settings (SNS_CG). The scale represents a possible minimum score of 1 indicating a low level of SNS privacy settings, and a maximum score of 5 indicating a high level of SNS privacy settings. The mean score for SNS privacy settings variable was 2.57 with a standard deviation of 1.57.

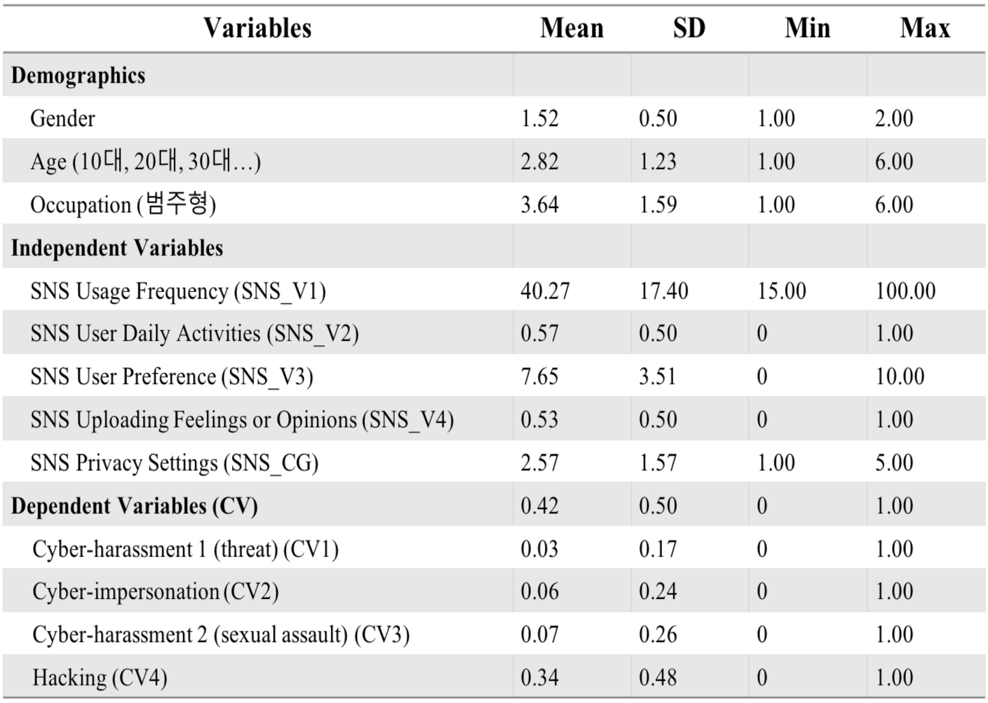
The measures were designed referring to the survey items that former studies have utilized to assess the lifestyle activities through SNS (Back, 2016; K. Choi, & Lee, J. R., 2017; Phillips, 2015). Although the mentioned studies have included 'risky online activities and behaviors' as a separate variable, this study does not regard those behaviors independently due to the specific characteristics of social networking sites. Users' activities do not clearly differ by vocational/leisure/risky activities on SNS.

Dependent Variables

There are four dependent variables in total to be assessed regarding cybercrime victimization (CV): *(violent) cyber-harassment (CV1), cyber-impersonation (CV2), (sexual) cyber-harassment (CV3), and hacking (CV4)*. As mentioned previously in the theoretical application section where the types of cybercrime are described in detail, this study focuses on the two legal categories classified by Wall's (2001), 'cyber-trespass' and 'cyber-violence'. The two types of cyber-harassment (violent and sexual) refer to cyber-violence and cyber-impersonation and hacking refer to cyber-trespass. The four dependent variables fall under the cybercrime victimization variable (CV). Respondents were asked to answer either "yes" or "no" if they have been victimized by any of the cybercrimes mentioned (CV1 to CV4). Using a binary scale for each dependent variable, the items were summed to create one CV variable. If the respondent was victimized by any of the four cybercrimes, the response is "yes" (1) and, if the respondent was not victimized by any, the response is recorded as "no" (0).

First, for CV, the scale represents a possible minimum score of 0 indicating no victimization, and a maximum score of 1 indicating that the respondent has been victimized by any of the four cybercrimes. The mean score for CV was 0.42 with a standard deviation of 0.50. For CV1, the scale represents a possible minimum score of 0 indicating no violent cyber-harassment victimization, and a maximum score of 1 indicating that the respondent has been victimized by violent cyber-harassment. The mean score for CV1 was 0.03 with a standard deviation of 0.17. For CV2, the scale represents a possible minimum score of 0 indicating no violent cyber-impersonation victimization, and a maximum score of 1 indicating that the respondent has been victimized by violent cyber-impersonation. The mean score for CV2 was 0.06 with a standard deviation of 0.24. For CV3, the scale represents a possible minimum score of 0 indicating no sexual cyber-harassment victimization, and a maximum score of 1 indicating that the respondent has been victimized by sexual cyber-harassment. The mean score for CV3 was 0.07 with a standard deviation of 0.26. For CV4, the scale represents a possible minimum score of 0 indicating no hacking victimization, and a maximum score of 1 indicating that the respondent has been victimized by hacking. The mean score for CV4 was 0.34 with a standard deviation of 0.48.

The descriptive statistics for study measures including the demographic variables, the independent variables, and the dependent variables are described in Table 2.



Variables	Mean	SD	Min	Max
Demographics				
Gender	1.52	0.50	1.00	2.00
Age (10대, 20대, 30대…)	2.82	1.23	1.00	6.00
Occupation (범주형)	3.64	1.59	1.00	6.00
Independent Variables				
SNS Usage Frequency (SNS_V1)	40.27	17.40	15.00	100.00
SNS User Daily Activities (SNS_V2)	0.57	0.50	0	1.00
SNS User Preference (SNS_V3)	7.65	3.51	0	10.00
SNS Uploading Feelings or Opinions (SNS_V4)	0.53	0.50	0	1.00
SNS Privacy Settings (SNS_CG)	2.57	1.57	1.00	5.00
Dependent Variables (CV)	0.42	0.50	0	1.00
Cyber-harassment 1 (threat) (CV1)	0.03	0.17	0	1.00
Cyber-impersonation (CV2)	0.06	0.24	0	1.00
Cyber-harassment 2 (sexual assault) (CV3)	0.07	0.26	0	1.00
Hacking (CV4)	0.34	0.48	0	1.00

Table. 2 Descriptive Statistics for Study Measures

4. Analysis & Results

Analysis

All dependent variables are binary since the responses were counted based on dichotomous scales. Since the nature of the dependent variable is binary, logistic regression analysis was considered to be the most appropriate technique. The following models describe how logistic regression analyses were carried out depending on the hypotheses, as in the independent variables.

For Hypothesis 1:

$$\ln(CV) = \beta 0 + \beta 1 x 1(SNS\_V1) + \beta 2 x 2(SNS\_V2) + \beta 3 x 3(SNS\_V3) + \beta 4 x 4(SNS\_V4) + \varepsilon$$

First, in order to find out whether the chosen independent variables, SNS usage frequency (SNS_V1), disclosing daily activities through SNS (SNS_V2), disclosing individual preference through SNS (SNS_V3), exposing feelings and opinions on SNS (SNS_CV4), are related to cybercrime victimization as a whole, the dependent variable CV was analyzed. Furthermore, in order to find out which cybercrime was related to the independent variables, the logistic regression model was analyzed with each separate dependent variable (CV1 to CV4).

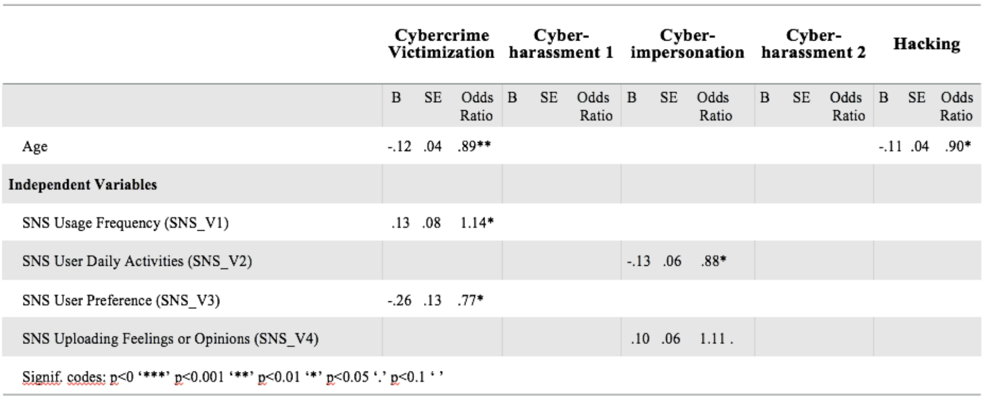
For Hypothesis 2:

$$\ln(CV) = \beta 0 + \beta 1 x 1(SNS\_CG) + \varepsilon$$

Then, in order to find out whether the SNS privacy settings as a capable guardianship was related to cybercrime victimization, the above regression model was used. Here, the different dependent variables from CV1 to CV4 were not necessarily considered meaningful to be analyzed separately.

Results

The current study yielded 4 significant findings regarding the relationship between elements of LRAT and cybercrime victimization and 2 significant findings regarding one of the demographic characteristics, age, and cybercrimes. In this section, the results will be presented by introducing the independent variables and discussing the significant relationships that each had with the respective cybercrimes. The independent variables related to the SNS lifestyle exposure activities and/or the demographic variable with the respective cybercrime that were found significantly related will be presented. The significant results based on the logistic regression analysis can be seen in Table 3.



	Cybercrime Victimization			Cyber-harassment 1			Cyber-impersonation			Cyber-harassment 2			Hacking		
	B	SE	Odds Ratio	B	SE	Odds Ratio	B	SE	Odds Ratio	B	SE	Odds Ratio	B	SE	Odds Ratio
Age	-.12	.04	.89**										-.11	.04	.90*
Independent Variables															
SNS Usage Frequency (SNS_V1)	.13	.08	1.14*												
SNS User Daily Activities (SNS_V2)							-.13	.06	.88*						
SNS User Preference (SNS_V3)	-.26	.13	.77*												
SNS Uploading Feelings or Opinions (SNS_V4)							.10	.06	1.11 .						
Signif. codes: p<0 '***' p<0.001 '**' p<0.01 '*' p<0.05 '.' p<0.1 ' '															

Table. 3 Inferential Statistics: Logistic Regression

Age/SNS Usage Frequency/SNS User Preference & Cybercrime Victimization

The first independent variable related to the SNS lifestyle exposure activities, SNS usage frequency, was operationalized as an individual's time and frequency for using any type of SNS. When this variable was intercepted with the demographic variable of age, it was found to have a significant effect on the likelihood of cybercrime victimization. Here, the cybercrime victimization represents the victimization of any of the four cybercrimes. According to this result, older individuals are approximately 11% less likely to be victimized by any cybercrime than the younger individuals (b= -0.12, Odds Ratio= 0.89). Individuals who use SNS more frequently are approximately 14% more likely to be victimized by any cybercrime than those who do not often use SNS (b= 0.13, Odds Ratio= 1.14). Lastly, individuals who disclose their preferences through SNS are approximately 23% less likely to be victimized by any cybercrime than those who do not disclose preferences through SNS (b= -0.26, Odds Ratio= 0.77). This is an unexpected result since it was first hypothesized that individuals who disclose preference would be more likely to be victimized. The importance and meaning of these findings will be discussed further in the discussion section of this paper.

Uploading User Daily Activities / Feelings or Opinions on SNS & Cyber-impersonation

The independent variable of SNS user daily activities refers to whether the individual discloses his or her daily activities via SNS and SNS uploading feelings or opinions refers to the willingness of an individual to share his or her feelings or opinions on SNS. Disclosing daily activities through SNS was found to be significantly related to cyber-impersonation. However, according to the result, those who disclose daily activities on SNS are 12% less likely to be victimized by such cybercrime (b= -0.13, Odds Ratio= 0.88). This is opposite to the hypothesis that individuals who share daily activities on SNS are more likely to be victims of cybercrime. On the other hand, those who upload feelings or opinions on their SNS are 11% more likely to be victimized by cyber-impersonation (b= -0.10, Odds Ratio= 1.11).

Age & Hacking

The result shows that the demographic variable, age, is significantly related to hacking. According to this result, respondents who are older are about 10% less likely to be victimized by hacking (b= -0.11, Odds Ratio= 0.90). This result, along with the relationship of age with cybercrime victimization as a whole, may be interpreted that individuals who are older are less likely to be victimized by hacking since they spend less time online.

Capable Guardianship – SNS Privacy Settings

The LRAT concept of capable guardianship was operationalized as one variable, SNS privacy settings. This independent variable was not found to have a significant effect on any of the observed cybercrimes.

5. Discussion

The current study sought to explore how SNS lifestyle exposure activities and the absence of digital capable guardianship affect the likelihood of cybercrime victimization of individuals via self-report survey responses. The four cybercrimes that were studied include threatening/violent cyber-harassment, cyber-impersonation, sexually assaulting cyber-harassment, and hacking. This study hypothesized that SNS activities that expose lifestyles and less strict privacy settings would increase the likelihood of cybercrime victimization.

The logistic regression analysis yielded six significant results and, in this section, the results will be discussed relative to the original hypotheses as well as possible implications. Next, limitations of the study as well as some suggestions for future research will be explored.

According to the findings of this study, the LRAT elements that had significant effects on the likelihood of cybercrime victimization included age, SNS usage frequency, exposure of daily activities through SNS, exposure of preference through SNS, and sharing feelings or opinions on SNS. Some results are consistent with the original hypotheses whereas others do not support them. Among the results, those that are consistent with the presented hypotheses are the following: individuals who use SNS more frequently are more likely to be victimized by any cybercrime than those who do not often use SNS and, those who share feelings or opinions through SNS are more likely to be victimized by cyber-impersonation. The unexpected results were the following: individuals who disclose daily activities or preferences on their SNS profiles are *less* likely to be victimized.

The current study is important to current and emerging literature because researchers and policymakers or even companies can use this information to understand the lifestyle factors that may contribute to cybercrime victimization. By analyzing these factors, education and prevention policy efforts can be made to reduce the risk of victimization and therefore make the internet a safer place for individuals to engage in their daily routine activities, such as social networking and communicating with others. Also, this study included different types of SNS platforms rather than focusing on only one.

Focusing more on the unexpected findings, there may be several explanations for such inconsistency between the original hypotheses and the results. The first significant finding negatively correlated with cybercrime victimization refers to individuals who disclose their preferences through SNS and that they are approximately 23% *less* likely to be victimized by any cybercrime than those who do not disclose preferences through SNS. Furthermore, the current study found that age matters as well. Older individuals are approximately 11% less likely to be victimized by any cybercrime than the younger individuals. These results indicate that younger individuals who use SNS and those who do not disclose preferences are more vulnerable to cybercrime. The original hypothesis stated that those who share more about their preferences through SNS are more likely to be victimized by cybercrimes. However, the result shows the opposite. This is meaningful since it can be interpreted that people may still be vulnerable to cybercrimes even though they do not actively show what they are interested in on SNS. Also, it could be interpreted that it might be easier for the offenders to target those who are less actively engaged on SNS or that a moderate level of use of social media may be sufficient to become a vulnerable target.

The second inconsistent result regarded as another significant finding was that individuals who disclose daily activities on SNS are 12% *less* likely to be victimized by cyber-impersonation. It is ironic since one could hypothesize that more disclosure would attract more cybercrimes but, it could also be interpreted as less disclosure invokes more curiosity. Additionally, the insufficient response data could be another potential explanation for such inconsistency of findings.

Another limitation of the current study is the limited types of cybercrime. This study only investigates those who were the victims of four types of cybercrime which are violent or sexually assaulting cyber-harassments, cyber-impersonation, and hacking. However, there may be individuals who were victimized by other cybercrimes such as cyber-stalking, sexting or other kinds of sexual assault online. The scope of cybercrime can be defined more broadly in future research.

There are opportunities for future research regarding possible privacy policy changes within social media companies. As most of the SNS companies make revenue by providing ad products to other companies, it is crucial for them to acquire more online users as well as maintaining them on their services. Therefore, as a researcher, it would be meaningful to find out the effect of cybercrime victimization on the users thus, whether or not being victims of cybercrimes would make them leave the platform. There would be useful managerial implications if future research focused on possible policy changes on SNS users' privacy settings.

6. Conclusion

With growing concerns about big social media firms already possessing already massive personal data, the current study adds more importance to exploring the possible outcomes of using social media carelessly. Not only should the individuals be more cautious about which personal information to share but also, the SNS companies need to find discrete solutions to protect their users. According to an article from the Economist, a report found that "there is a growing range of new job opportunities in the fields of big data analysis, …, and online chaperones ("managing online risks such as identity theft, reputational damage, social media bullying and harassment, and internet fraud")." This meant that, as the gravity of the situation worsens, people are preparing for the consequences.

Using techniques supported by existing literature, this study applied LRAT to cybercrime victimization, specifically violent and sexually assaulting harassments, impersonation, and hacking, by conducting a self-report survey. The current study found moderate support for the application of LRAT to cybercrime victimization. While the study yielded significant results, both consistent and inconsistent with the original hypotheses, it is important to keep in mind the limitations previously discussed. Hopefully, the current study will help develop the understanding of and literature on cybercrime victimization as well as encouraging further discussion on how to prevent such crimes from harming individuals.

7. References

Alshalan, A. (2006). *Cyber-Crime Fear and Victimization: An Analysis of a National Survey*. Mississippi.

Back, S. (2016). *Empirical Assessment of Cyber Harassment Victimization via Cyber-Routine Activities Theory.* (Master of Criminal Justice), Bridgewater State University.

Cappadocia, M. C., Craig,W., & Pepler, D. (2013). Cyberbullying: Prevalence, stability, and risk factors during adolescence. *Canadian Journal of School Psychology, 28*, 171-192.

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Choi, K., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending 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 activities approach. *American Sociological Review, 44*(4), 588-608.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predator victimization: An exposition and test of a formal theory. *American Sociological Review, 46*, 505-524.

Dredge, R., Gleeson, J., & de la Piedad Garcia, X. (2014). Presentation on Facebook and risk of cyberbullying victimisation. *Computers in Human Behavior, 40*, 16-22.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity theory approach. *Theory and Practice in Situational Crime Prevention, Crime Prevention Studies, 16*, 7-39.

Elias, R. (1986). *The politics of victimization: victims, victimology, and huma rights*: New York: Oxford Press.

Halder, D., & Jaishankar, K. (2011). *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations*. India: Manonmaniam Sundaranar University.

Henson, B., Reyns, B. W., & Fisher, B. S. (2011). Security in the 21st century examining the link between online social network activity, privacy, and interpersonal victimization. *Criminal Justice Review, 36*(3), 253-268.

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

Hinduja, S., & Patchin, J. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior, 29*, 129-156.

Holt, T. J., & Bossler, A. M. (2009). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior, 30*, 1-25.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*, 189-220.

Kokkinos, C. M., & Saripanidis, I. (2017). A lifestyle exposure perspective of victimization through Facebook among university students. Do individual differences matter? *Computers in Human Behavior, 74*, 235-245.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research

among youth. *Psychological Bulletin, 140*, 1073.

Messner, S. F., & Blau, J. R. (1987). Routine Leisure Activities and Rates of Crime: A Macro-Level Analysis. *Social Forces, 65*(4), 1035-1052.

Miethe, T. D., & Meier, R. F. (1994). *Crime and its social context : toward an integrated theory of offenders, victims, and situations.*: Albany: State University of New York Press.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773.

Peluchette, J. V., Karl, K., Wood, C., & Williams, J. (2015). Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem? *Computers in Human Behavior, 52*, 424-435.

Phillips, E. (2015). *Empirical Assessment of Lifestyle-Routine Activity and Social Learning Theory on Cybercrime Offending.* (Master of Criminal Justice), Bridgewater State University.

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.

Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428-438.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society, 4*(1), 71-92.

Staksrud, E., Olafsson, K., & Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior, 29*, 40-50.

Svensson, R., & Pauwels, L. (2010). Is a risky lifestyle always “risky”? The interaction between individual propensity and lifestyle risk in adolescent offending: A test in two urban samples. *Crime & Delinquency*, 608-626.

Wall, D. (2001). *Cybercrimes and the internet. In D. Wall (ed.) Crime and the internet*: London: Routledge.

Walrave, M., & Heirman, W. (2011). Cyberbullying: Predicting victimization and perpetration. *Children & Society, 25*, 59-72.

Wearesocial. (2017). Digital in 2017: Global Overview. Retrieved from https://wearesocial.com/special-reports/digital-in-2017-global-overview

Wilson, R. E., Gosling, S. D., & Graham, L. T. (2012). A review of Facebook research in the social sciences. *Perspectives on Psychological Science, 7*, 203-220.

Yar, M. (2005). The novelty of ‘cybercrime’ an assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.

Yucedal, B. (2010). *Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories.* (Doctor of Philosophy), Kent State University.

8. Appendix: Survey Questionnaire

SNS Lifestyle Exposure Activities and Cybercrime Victimization Survey

Dear respondent,

Thank you for kindly spending your time for this survey.

This survey targets those who are subscribed to any of the main 5 SNS platforms (Facebook, Instagram, KakaoStory, Naver Band, and Twitter) chosen for the research.

It is constituted with 4 separate parts: Demographics, SNS lifestyle exposure activities, SNS capable guardianship, cyber victimization. You can skip the questions not required to answer if it does not concern you. There is no right or wrong answer for any of the questions. Please feel free to answer based on your personal experience and opinions. This survey is not used for any other purpose than the research.

Thank you.

Sincerely,

Jiseon Choe from Seoul National University
Management of Information Systems (MIS) Masters candidate

Contact information: jschoe03@snu.ac.kr

Part I. Demographics

Instructions: Please complete the section below by filling in or checking off the selection that best suits you.

1. What is your gender?

   ( ) Male
   ( ) Female

2. What is your age? (Korean age)

   ( ) 10 ~ 19
   ( ) 20 ~ 29
   ( ) 30 ~ 39
   ( ) 40 ~ 49
   ( ) 50 ~ 59
   ( ) 60 ~

3. What is your occupation?

   ( ) Engineering / technician / IT-related
   ( ) Student
   ( ) Art / entertainment / sports
   ( ) Business management / finance
   ( ) Education / research / law / medical
   ( ) Other ___________

Part II. SNS Lifestyle Exposure Activities

Instructions: The following questions focus on your SNS activities. Please check or write in the appropriate answer.

1. Which SNS accounts are you subscribed to? (multiple responses possible)

   ( ) Facebook

(   ) Instagram
(   ) KakaoStory
(   ) Naver Band
(   ) Twitter
(   ) Other ___________

2. Which SNS platforms do you use most often in order to write postings, comments, and to follow pages or public figures? (multiple responses possible)

   (   ) Facebook
   (   ) Instagram
   (   ) KakaoStory
   (   ) Naver Band
   (   ) Twitter
   (   ) Other ___________

3. Which device do you use the most in order to connect to SNS?

   (   ) Smartphone
   (   ) Tablet / iPad
   (   ) Desktop PC / Laptop
   (   ) Public computer

4. Is there a specific time of the day for using SNS?

   (   ) Specific time (e.g., when going to work, or way back home)
   (   ) Randomly (e.g., whenever I feel like it or have the time to)

5. On average, how much time do you spend on SNS in a day? (Please write specific amount of minutes spent and check the appropriate answer below)

   _____ mins. on average

   (   ) 0 ~ 30 mins.
   (   ) 30 mins. ~ 1 hour
   (   ) 1 ~ 2 hours
   (   ) 2 ~ 3 hours

( ) 3 ~ 4 hours
( ) 4 ~ 5 hours
( ) more than 5 hours

6. On average, how many photos, video clips, or postings (text) do you upload on SNS in a week? (including sharing postings) (Please write the number where appropriate)

	0	1 ~ 5	6 ~ 10	11 ~
Facebook				
Instagram				
KakaoStory				
Naver Band				
Twitter				

7. On average, how many comments do you write on SNS in a week? (Please write the number where appropriate)

	0	1 ~ 5	6 ~ 10	11 ~
Facebook				
Instagram				
KakaoStory				
Naver Band				
Twitter				

8. Do you share your daily activities on SNS?

( ) Yes
( ) No

9. Do you share your feelings or opinions through SNS?

( ) Yes
( ) No

10. What type of contents are included in most of your postings? (multiple responses possible)

( ) Family, friends, or acquaintances
( ) Work place, school, residential area
( ) Valuable products you own (e.g., bag or watch from luxury brands, automobiles, etc.)
( ) Body shape (e.g., photo wearing a bikini, tight clothes)
( ) Scenery, food, animals
( ) Opinions, feelings
( ) Other ___________

11. Do you 'follow' the profile (e.g., artists or public figures)/page that you like or are interested in?

( ) Yes
( ) No

12. Do you 'like' the postings that you like or are interested in?

( ) Yes
( ) No

13. Have you ever accepted a friend request from someone you do not know personally?

( ) Yes
( ) No

14. Do you 'follow' or leave comments to the pages/profiles that have risky contents (e.g., information on hacking, terrorism, pornography, etc.)?

( ) Yes
( ) No

Part III. SNS Capable Guardianship

Instructions: The following questions focus on your SNS privacy settings. Please check or write in the appropriate answer.

1. I let strangers (people who I am not ‘friends’ with) access my SNS profile (postings, friends network, or activities).

Strongly disagree				Strongly agree
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

2. I update my SNS privacy settings often.

Strongly disagree				Strongly agree
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

Part IV. Cybercrime Victimization

Instructions: The following questions focus on your cybercrime victimization. Please check or write in the appropriate answer.

A. Violent Cyber-harassment

A-1. Have you ever received threatening or violent messages (direct message or e-mail)?

(   ) Yes
(   ) No

A-2. If yes, when was it? (e.g., 3 weeks ago, 1 year ago)

____

A-3. If yes, what was it about?

____

A-4. "I felt it very threatening."

Strongly disagree				Strongly agree
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

A-5. "I felt unpleasant."

Strongly disagree				Strongly agree
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

A-6. How did you cope with it?

( ) I ignored it.
( ) I reacted in a similar way with what the offender has done.
( ) I reported it to the police.
( ) I closed my SNS account.
( ) I left my account but did not upload any new postings.
( ) Other ____________

A-7. Have you been victimized again in a similar way afterwards?

( ) Yes
( ) No

B. Cyber-impersonation

B-1. Have you ever been impersonated by another person online?

( ) Yes
( ) No

B-2. If yes, when was it? (e.g., 3 weeks ago, 1 year ago)

____

B-3. If yes, what was it about?

____

B-4. "I felt it very threatening."

Strongly disagree agree				Strongly
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

B-5. "I felt unpleasant."

Strongly disagree agree				Strongly
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

B-6. How did you cope with it?
( ) I ignored it.
( ) I reacted in a similar way with what the offender has done.
( ) I reported it to the police.
( ) I closed my SNS account.
( ) I left my account but did not upload any new postings.
( ) Other ___________

B-7. Have you been victimized again in a similar way afterwards?

( ) Yes

( ) No

C. Sexual Cyber-harassment

C-1. Have you ever received illegal sexual contents or messages (direct message or e-mail)?

( ) Yes
( ) No

C-2. If yes, when was it? (e.g., 3 weeks ago, 1 year ago)

____

C-3. If yes, what was it about?

____

C-4. "I felt it very threatening."

Strongly disagree				Strongly agree
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

C-5. "I felt unpleasant."

Strongly disagree				Strongly agree
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

C-6. How did you cope with it?
( ) I ignored it.
( ) I reacted in a similar way with what the offender has done.
( ) I reported it to the police.
( ) I closed my SNS account.
( ) I left my account but did not upload any new postings.

( ) Other ___________

C-7. Have you been victimized again in a similar way afterwards?

( ) Yes
( ) No

D. Hacking

D-1. Have you ever been hacked?

( ) Yes
( ) No

D-2. If yes, when was it? (e.g., 3 weeks ago, 1 year ago)

____

D-3. If yes, what was it about?

____

D-4. "I felt it very threatening."

Strongly disagree				Strongly agree
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

D-5. "I felt unpleasant."

Strongly disagree				Strongly agree
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

D-6. How did you cope with it?

(   ) I ignored it.
(   ) I reacted in a similar way with what the offender has done.
(   ) I reported it to the police.
(   ) I closed my SNS account.
(   ) I left my account but did not upload any new postings.
(   ) Other ___________

D-7. Have you been victimized again in a similar way afterwards?

(   ) Yes
(   ) No

E. Other Type of Cybercrime

E-1. Have you ever been victimized online by any means?

(   ) Yes
(   ) No

E-2. If yes, when was it? (e.g., 3 weeks ago, 1 year ago)

____

E-3. If yes, what was it about?

____

E-4. "I felt it very threatening."

Strongly disagree				Strongly agree
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

E-5. "I felt unpleasant."

Strongly disagree agree				Strongly
( ) 1	( ) 2	( ) 3	( ) 4	( ) 5

E-6. How did you cope with it?

(   ) I ignored it.
(   ) I reacted in a similar way with what the offender has done.
(   ) I reported it to the police.
(   ) I closed my SNS account.
(   ) I left my account but did not upload any new postings.
(   ) Other ___________

E-7. Have you been victimized again in a similar way afterwards?

(   ) Yes
(   ) No

요약(국문초록)

인터넷이란 공간의 무한한 가능성은 사회활동 및 여가활동과 관련된 개개인의 생활양식(라이프스타일)에 큰 변화를 일으켜왔다. 페이스북 또는 인스타그램과 같은 소셜네트워크서비스들은 상호교류를 하기에는 적합한 환경이지만, 반면에 동기부여가 된 범법자들이 범죄를 저지르기에도 매우 적합한 환경이기 때문에 개개인이 더욱 취약한 상황에 놓인다. 이 연구의 목적은 사이버공간에서의 괴롭힘, 사칭, 해킹 등의 사이버범죄들로 인한 피해 발생에 대해 조사하는 것이다. 로지스틱 회귀분석으로 100 여명의 응답자를 대상으로 한 설문조사를 통해 수집한 데이터를 분석하여 SNS 상에서의 생활양식 노출 활동들과 사이버 범죄 피해 간에 어떠한 관계가 있을지 연구하였다. 분석 결과에 따르면, 생활양식-일상활동이론(LRAT)이 적정 수준 적용된다는 점을 파악할 수 있었다. 문제 해결을 위한 교육 방안과 경영 차원에서의 함의 그리고, 추후 연구를 위해 몇 가지 제안사항들을 언급하면서 마친다.

키워드: 생활양식-일상활동이론(LRAT), 라이프스타일, 사이버범죄, 사이버범죄 피해, SNS, 온라인 사용자 행동

학번: 2016-20634